Atop Technologies, Inc.

Industrial Smart Secure Layer-2 Switch

User Manual

V1.7

September 29th, 2022

This PDF Document contains internal hyperlinks for ease of navigation.
For example, click on any item listed in the Table of Contents to go to that page.

Published by:

Atop Technologies, Inc.

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City, Hsinchu County
Taiwan, R.O.C.

Tel: +886-3-550-8137
Fax: +886-3-550-8131
www.atoponline.com
www.atop.com.tw

Important Announcement

Disclaimer

We have checked the contents of this manual for agreement with the hardware and the software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual is reviewed regularly and any necessary corrections will be included in subsequent editions.
Suggestions for improvement are welcome. All other product's names referenced herein are registered trademarks of their respective companies.

Preface

This manual contains some advanced network management knowledge, instructions, examples, guidelines, and general theories. The contents are designed to help users manage the switch and use its software, a background in general theory is a must, when reading it. Please refer to the Glossary for technical terms and abbreviations.

Who Should Use This User Manual

This manual is to be used by qualified network personnel or support technicians who are familiar with network operations and might be useful for system programmers or network planners as well. This manual also provides helpful and handy information for first time users. For any related problems, please contact your local distributor. If they are unable to assist you, please redirect your inquiries to www.atop.com.tw.

Warranty Period

Atop technology provides a limited 5-year warranty for unmanaged Ethernet switches.

Documentation Control

Author:	Shawn Wu
Revision:	1.7
Revision History:	Updated
Creation Date:	1 September 2017
Last Revision Date:	29 September 2022
Product Reference:	Layer-2 Managed Smart Secure Switch EHG2408 series
Document Status:	Released

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Introduction to Industrial Smart Switch

ATOP's EHG (Ethernet Switching Hub Full Gigabit, or Fast Ethernet Switching Hub) 24XX series are product lines of powerful industrial switch which are referred to as Open Systems Interconnection (OSI) Layer 2 bridging devices.

ATOP's switch is also an industrial switch and not a typical commercial switch. A commercial switch simply works in a comfortable office environment. However, an industrial switch is designed to perform in harsh industrial environments, i.e., extreme temperature, high humidity, dusty air, potential high impact, or the presence of potentially high static charges. Atop's unmanaged switch works fine even in these environments.

ATOP's switch supports essential IEEE standard protocols. This switch is excellent for keeping systems running smoothly, reliable for preventing system damage or losses, and friendly to all levels of users. The goal of this innovative product is to bring users an easy network management experience with robustness.

This device also embeds advanced encryption protocols in order to have the link on 2 Gigabit ports to be encrypted through 802.1AE MACSec Protocol. This protocol, working on Layer-2, encrypts hop-to-hop the data flow through a dedicated hardware that guarantees ultra-low-latency and throughput up to 98% with large packet sizes. The throughput can't achieve a theoretical 100% of non-encrypted because of the fact that MACSec headers make the packet longer.

1.2 Software Features

ATOP's Industrial Layer-2 Smart Secure Switches come with essential network protocols and software features. These protocol and software features allow the network administrator to implement security and reliability into their network with ease. These features enable Atop's switches to be used in safety applications, and factory and process automation. The followings are the list of protocols and software features.

- User Interfaces
  - Web browser
- Dynamic Host Configuration Protocol (DHCP) Client
- Security
  - Media Access Control Security (MACSec) or IEEE 802.1AE standard
- Layer-2 Switching
- Time Synchronization
  - Network Time Protocol (NTP) Server/Client
  - Simplified Network Time Protocol (SNTP)
- Mirror Port
- Simple Network Management Protocol (SNMP) v1/v2/v3 (with MD5 Authentication and DES encryption)
- SNMP Inform
- Rapid Spanning Tree Protocol (RSTP)
- Virtual Local Area Network (VLAN)
- IEEE 802.1x / Extensible Authentication Protocol (EAP) / Remote Authentication Dial-In User Service (RADIUS)
- Link Layer Discovery Protocol (LLDP)
- Alarm System (E-mail Notification)

2 Configuring with a Web Browser

Chapter 2 explains how to access the industrial smart switch for the first time by using the web browser.
The web browser allows users to access the switch over the Internet or the Ethernet LAN which has a user-friendly interface.

2.1 Web-based Management Basics

Users can access the smart secure switch easily using their web browsers (Internet Explorer 8 or 11, Firefox 44, Chrome 48 or later versions are recommended). We will proceed to use a web browser to introduce the smart switch's functions.

2.1.1 Default Factory Settings

Below is a list of default factory settings. This information will be used during the login process. Make sure that the computer accessing the switch has an IP address in the same subnet and the subnet mask is the same. Table 2.1 summarizes the default IP setting for EHG2408 series.

IP Address: 10.0.50.1
Subnet Mask: 255.255.0.0
Default Gateway: 0.0.0.0
User Name: admin
Password: default

Table 2.1 Default Setting for IP Network on EHG2408 Series

Model Name	Default IP Setting			
	IP	Netmask	Gateway	Default DNS
EHG2408	10.0.50.1	255.255.0.0	0.0.0.0	0.0.0.0
EHG2408-2SFP	10.0.50.1	255.255.0.0	0.0.0.0	0.0.0.0

2.1.2 Login Process and Main Window Interface

Before users can access the configuration, they have to log in. This can simply be done in two steps.

1. Launch a web browser.
2. Type in the switch IP address (e.g. http://10.0.50.1), as shown in Figure 2.1).
   Note: After pressing the Enter key, the login page will be shown. User has to input the default password which is set to "default".

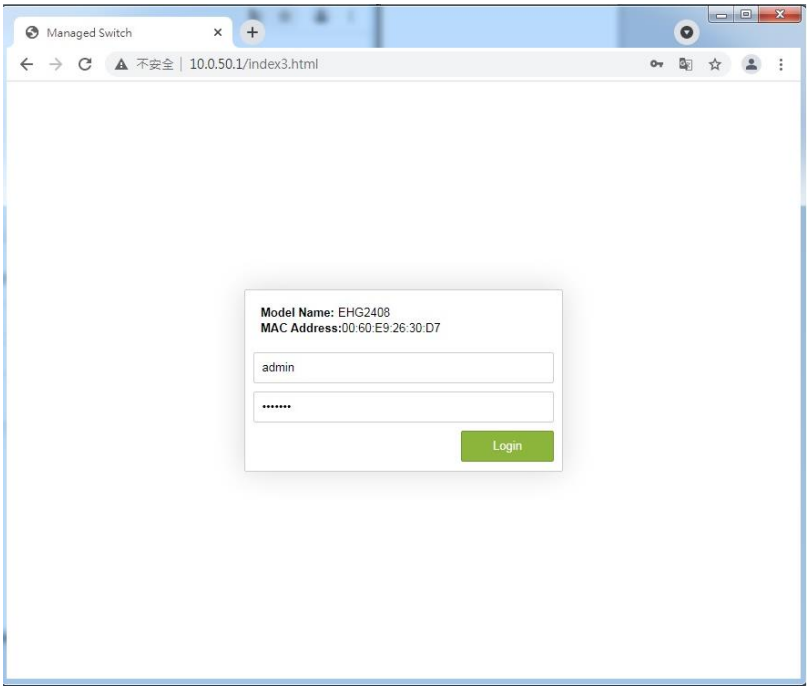

Figure 2.1 IP Address for Web-based Setting

After the login process, the main interface will show up for EHG2408 and EHG2408-2SFP, as shown in Figure 2.2 and Figure 2.3, respectively. The main menu (left side of the screen) provides the links at the top-level links of the menu hierarchy and by clicking on each item it allows lower-level links to be displayed. Note that the difference between EHG2408 and EHG2408-2SFP is that the EHG2408-2SFP will have **Port Setting** menu for its optical fiber slots.

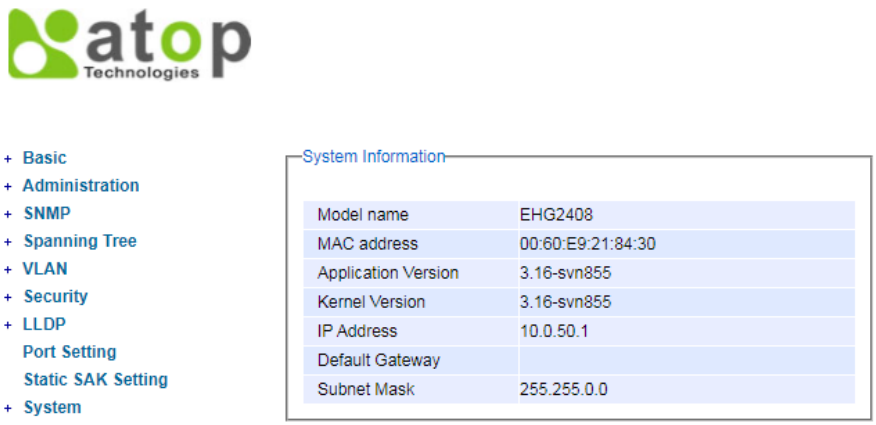

Figure 2.2 Default Web Interface of EHG2408

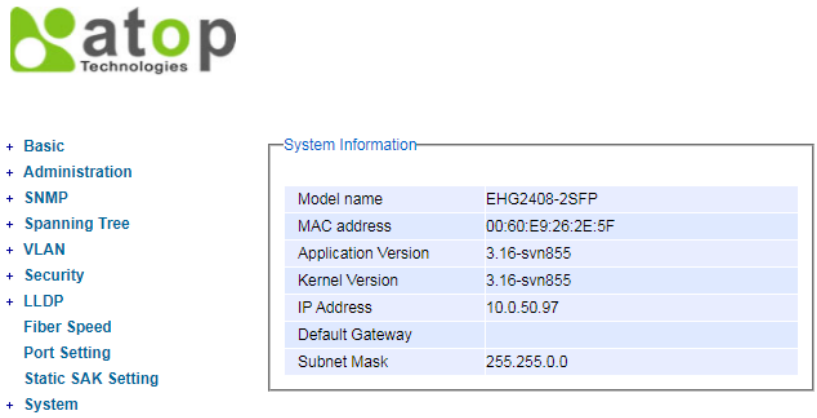

Figure 2.3 Default Web Interface of EHG2408-2SFP

2.2 Basic

2.2.1 System Info

To help users become familiar with the device, the **System Information** or **System Info** section provides important details of the ATOP's industrial smart secure switch. This is also the main welcome screen once the user has logged in. The details make it easier to identify different switches connected to the network. The user can check various information such as the **Model Name**, **MAC Address**, **Firmware Version**, **Kernel Version**, **IP Address**, **Default Gateway** and **Subnet Mask**. Figure 2.4 depicts an example of System Information of EHG2408. Table 2.2 summarizes the description of each field of system information.

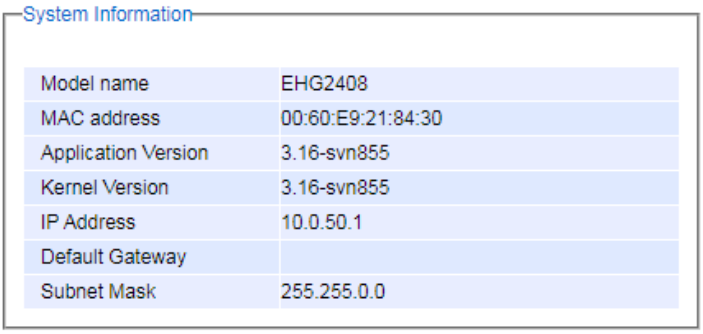

Figure 2.4 Details of System Info Webpage

Table 2.2 Descriptions of the Basic information

Label	Description
Model Name	The device's complete model name
MAC Address	The MAC address of the device
Firmware Version	The current firmware version of the device
Kernel Version	The current kernel version of the device
IP Address	The IP address to login into the configuration page of the device
Default Gateway	The current setting of the default gateway
Subnet Mask	The subnet mask for identified the network address of the device

2.2.2 System Setting

Users can assign device's details to Atop's switch in this section. By entering unique and relevant system information such as device name, this information can help identify one specific switch among all other devices in the network. Please click on the "**Update**" button to update the information on the switch. Figure 2.5 shows **Device Information Setting** page of an EHG2408 smart secure switch model. Table 2.3 summarizes the device information setting descriptions and corresponding default factory settings.

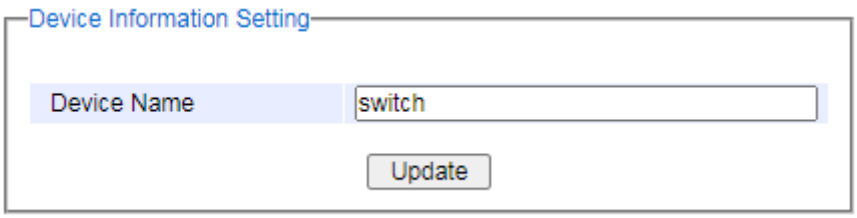

Figure 2.5 Details of System Setting Webpage

Table 2.3 Descriptions of the System Setting

Label	Description	Factory Default

Device Name	Specifies a particular role or application of different switches. The name entered here will also be shown in Atop's Device Management Utility. Max. 63 Char.	switch

2.3 Administration

2.3.1 Account

The users with administration access right can create and delete accounts through **Account** Section. As shown in Figure 2.6, there are total of four section boxes inside **Account** page as the followings: **Account list**, **Add account**, **Change password** and **Password strength configuration.** In **Account List** box (1st row of Figure 2.6), the users and their access rights are listed. There are two types of access right: **admin** and **user**. The **admin**'s access right has **read/write** permission on the managed switch while the **user**'s access right has only **read** permission. If the user with administration access right would like to delete any account, the user can select the account that would like to be deleted and click "**Delete**" button. Note that the user cannot delete his/her own account. The user whose account was deleted will be logged out immediately.

In the **Add account** box (2nd row of Figure 2.6), the user can input a username in the **Username** textbox as well as input a password in the **Password** textbox. Then the user can select an appropriate **Access Right** from the drop-down list for the user before clicking **Add** button. After clicking it, a new account will be created in the **Account List** box. A username "admin" with an "admin" **Access Right** is created as the default. The maximum number of accounts is 15 accounts.

If the user wishes to change password for any account, the user can do so in the **Change password** box (3rd row of Figure 2.6). Here, the user has to select a user name from the **Username** dropdown box first. Then, input a password that user would like to change it to in **New password** textbox before reentering the same password in the **Confirm password** textbox. The **Minimun length** and the **Maximum length** of each password can be configured through the **Password strength configuration** box in the last row of Figure 2.6.

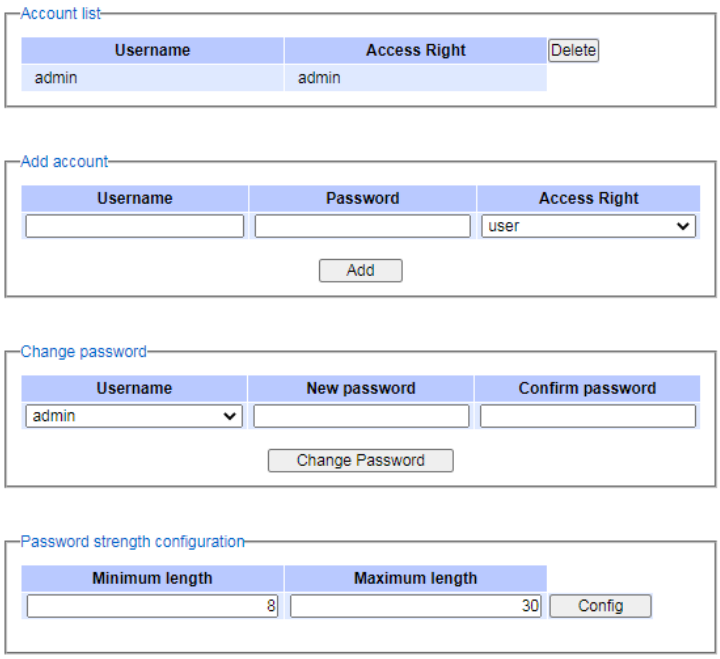

Figure 2.6 Account Setting Webpage

2.3.2 Connection

The **Connection** sub-menu under the **Account** menu lists the users who currently access the device under the **Connection Management** box. Inside the box, the table lists the information of the users with four columns: **Username**, **Access Right**, **Session**, and **Source IP** is shown in Figure 2.7 錯誤! 找不到參照來源。.

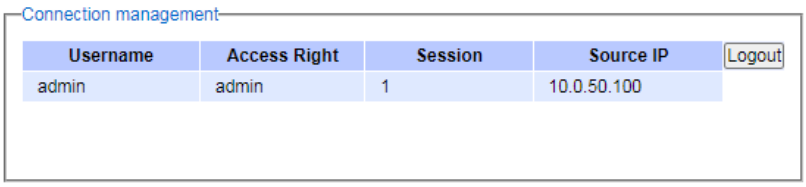

Figure 2.7 Connection Management Webpage

2.3.3 Auth Server Setting

In addition to the local authentication, the switch can be configured to request for authentication through a centralized RADIUS Server when the local authentication fails. Figure 2.8 shows the setting parameters for authentication server while Table 2.4 summarizes the authentication server settings.

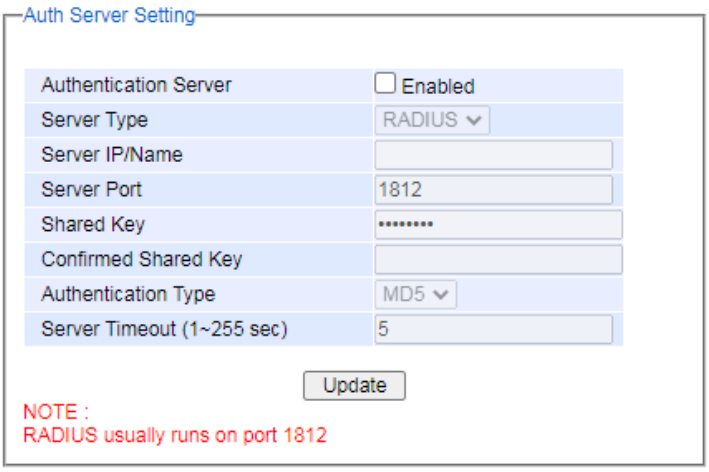

Figure 2.8 Authentication Server Setting

Table 2.4 Descriptions of Authentication Server Settings

Label	Description	Factory Default
Authentication Server	Enable/ Disable authentication through a remote authentication server	Disabled
Server Type	Choose Authentication Server type: RADIUS. See notes below for a detailed explanation.	RADIUS
Server IP/Name	IP address of the authentication server	NULL
Server Port	Communication port of the authentication server	1812
Shared Key	The key used to authenticate with the server. Max 15 characters.	12345678
Confirmed Shared Key	Re-type the shared key. Max 15 characters.	NULL
Authentication Type	Authentication mechanism. MD5.	MD5
Server Timeout (1~255 sec)	The time out period of waiting for a response from the authentication server. This will affect the time that the next login prompt shows up in case that the server is not available.	5

When configuring RADIUS as the authentication server, the system administrator of the RADIUS server must also make sure that the RADIUS's service-type attribute of each new user matches that particular user. For example, if a user has an administrative right that user should have read/write privilege, this user should be set Service-Type attribute on RADIUS server as "Administrative-User". On the other hand, if a user has only normal privilege that is only read permission, this user should be set Service-Type attribute on RADIUS server as "NAS-Prompt-User". Note

that NAS is refered to Network Access Server or the EHG2408 Switch in this case. NAS is a client of RADIUS server. Depicts an example of a user called "admin1" with Cleartext-Password attribute of "default1" and Service-Type attribute of "Administrative-User".

*NOTE:
RADIUS (Remote Authentication Dial in User Service):
RADIUS is an access server that uses authentication, authorization, and accounting (AAA) protocol for authentication and authorization. It is a distributed security system that secures remote access to networks and network services against unauthorized access. The RADIUS specification is described in RFC 2865, which obsoletes RFC 2138.

2.3.4 IP Setting

The **IP Setting** webpage is depicted in Figure 2.9. Inside the **Local Login Setting** box, the user can enable Dynamic Host Configuration Protocol (DHCP) client inside the switch by checking the **DHCP** box so that the switch can obtain IP address' setting automatically from a DHCP server available on the user's local network. If the DHCP is enabled, the rest of the fields will be disabled. Note that the user should consult your local network administrator for information about the availability of DHCP server. If the user prefers a static IP setting, then the user can proceed to enter the **IP Address**, **Subnet Mask**, **Gateway**, and the **Primary DNS**. If the user set gateway or DNS on this page, the smart secure switch will not use the gateway or the DNS from DHCP server. After entering the desired information, please click **Update** button to change the IP Setting.

The description of each field and its default value in IP Setting webpage are summarized in Table 2.5.

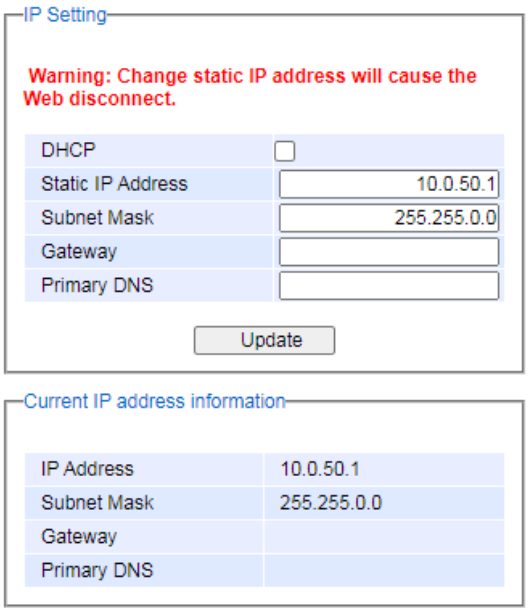

Figure 2.9 IP Setting Webpage

Table 2.5 Descriptions of IP Settings

Label	Description	Factory Default
DHCP	By checking this box, an IP address and related fields will be automatically assigned. Otherwise, users can set up the static IP address and related fields manually.	Uncheck
Static IP Address	Display current IP address. Users can also set a new static IP address for the device.	10.0.50.1
Subnet Mask	Display current Subnet Mask or users can set a new subnet mask in this field	255.255.0.0

Gateway	Show current Gateway or set a new IP address for the Gateway	0.0.0.0
Primary DNS	Set the primary DNS' IP address to be used by your network	NULL

2.3.5 Ping

Atop's managed switch provides a network tool called Ping for testing network connectivity in this subsection. Ping is a network diagnostic utility for testing reachability between a destination device and the managed switch. Note that this utility is only for IPv4 address. Figure 2.10 shows the user interface for using the Ping command.

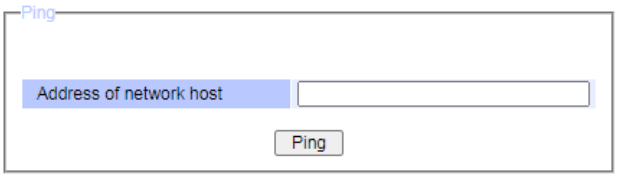

Figure 2.11 Ping Webpage

2.3.6 Mirror Port

Mirror Port is used on switches to send a copy of network packets sent/received on one switch port or a range of switch ports to a network monitoring connection on another switch port (Monitor Port).
Port mirroring is used in network systems that require monitoring of network traffic, such as an IDS ("Intrusion Detection System").
Port mirroring, together with an NTA ("Network Traffic Analyzer"), can help to monitor network traffic. Users can monitor the selected ports ("Source Ports") for egress and/or ingress packets.
• "Source Port": The incoming data packets are copied and forwarded to the monitor port.
• "Destination Port": The outgoing data packets are copied and forwarded to the monitor port.

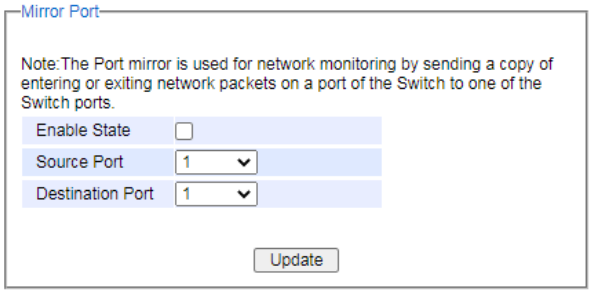

Figure 2.12 Mirror Port Webpage

2.3.7 System Time

Atop's industrial managed switch has internal calendar (date) and clock (or system time) which can be set manually or automatically. Figure 2.13 shows the System Time and SNTP webpage. The users have options to configure **Current Date** and **Current Time** manually. There is a drop-down list of **Time Zone** which can be selected for the local time zone. If the switch is deployed in a region where daylight saving time is practiced (see note below for explanation), please check the **Enable** option for **Daylight Saving Time**. Then, the users will have to enter the **Start Date**, **End Date**, and **Offset** in hour(s).

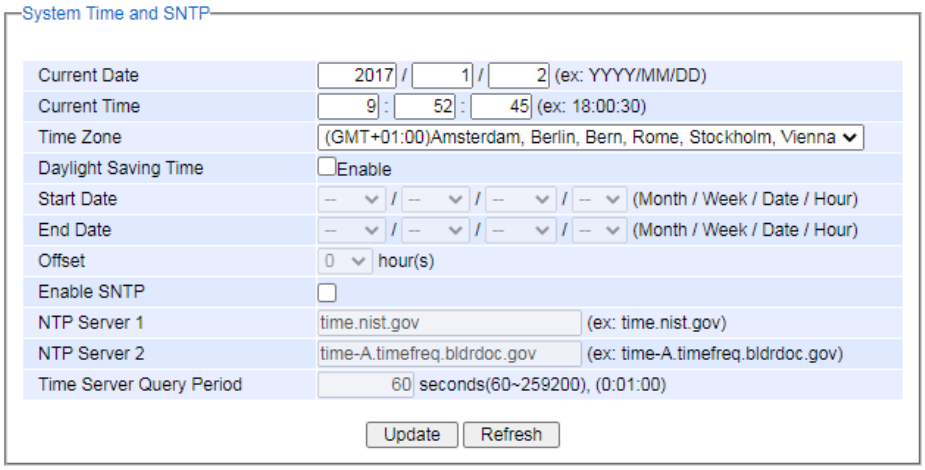

Figure 2.13 Webpage for Setting System Time and SNTP

For automatically date and time setting, the users can enable Simple Network Time Protocol (SNTP) by checking the **Enable SNTP** option (see note below for explanation). Then, the users must enter the NTP Server 1 and NTP Server 2 which will be used as the reference servers to synchronize date and time to. The users can specify the Time Server Query Period for synchronization which is in the order of seconds. The value for this period will depend on how much clock accuracy the users want the switch to be. Finally, the managed switch can become a network time protocol server for the local devices by checking the box behind the **Enable NTP Server** option. Description of each option is provided in Table 2.6.

Table 2.6 Descriptions of the System Time and the SNTP

Label	Description	Factory Default
Current Date	Allows local date configuration in yyyy/mm/dd format	None
Current Time	Allows local time configuration in local 24-hour format	None
Time Zone	The user's current local time	(GMT+01:00)
Daylight Saving	Enable or disable Daylight Saving Time function	Unchecked
Start Date	Define the start date of daylight saving	NULL
End Date	Define the end date of daylight saving	NULL
Offset	Decide how many hours to be shifted forward/backward when daylight saving time begins and ends. See note below.	0
Enable SNTP	**Enables SNTP** function. See note below.	Unchecked
NTP Server 1	Sets the first IP or Domain address of **NTP Server.**	time.nistgov
NTP Server 2	Sets the second IP or Domain address of NTP Server. Switch will locate the 2nd **NTP Server** if the 1st NTP Server fails to connect.	time-A.timefreq.bldrdoc.gov
Time Server Query Period	This parameter determines how frequently the time is updated from the NTP server. If the end devices require less accuracy, longer query time is more suitable since it will cause less load to the switch. The setting value can be in between 60 – 259200 (72 hours) seconds.	60

***Note:**

- Daylight Saving Time: In certain regions (e.g. US), local time is adjusted during the summer season in order to provide an extra hour of daylight in the afternoon, and one hour is usually shifted forward or backward.

- **SNTP**: **S**imple **N**etwork **T**ime **P**rotocol is used to synchronize the computer systems' clocks with a standard NTP server. Examples of two NTP servers are *time.nist.gov* and *time-A.timefreq.bldrdoc.gov.*

2.3.8 Modbus Setting

Atop's EHG2408 switch can be connected to a Modbus network using Modbus TCP/IP protocol which is an industrial network protocol for controlling automation equipment. The managed switch's status and settings can be read and written through Modbus TCP/IP protocol which operates similar to a Management Information Base (MIB) browser. The managed switch will be a Modbus slave which can be remotely configured by a Modbus master. The Modbus slave address must be set to match the setting inside the Modbus master. In order to access the managed switch, a **Modbus Address** must be assigned as described in this subsection. Figure 2.14 shows the Modbus Setting webpage, and Modbus memory mapping table lists all the register's addresses inside the managed switch and their descriptions, is provide in Table 2.7.

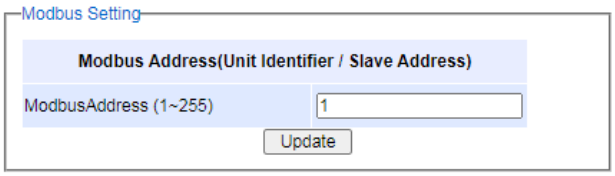

Figure 2.14 Modbus Setting Webpage

Table 2.7 Modbus Memory Map

Modbus	Address (Hex)	Length (Word)	Interpretation	Description
1080	0x438	12	ASCII	Firmware Version
1096	0x448	16	ASCII	Firmware Release Date
1112	0x458	3	HEX	Ethernet MAC Address
1256	0x4E8	1	HEX	Link Status of Port 1
1257	0x4E9	1	HEX	Link Status of Port 2
1258	0x4EA	1	HEX	Link Status of Port 3
1259	0x4EB	1	HEX	Link Status of Port 4
1260	0x4EC	1	HEX	Link Status of Port 5
1261	0x4ED	1	HEX	Link Status of Port 6
1262	0x4EE	1	HEX	Link Status of Port 7
1263	0x4EF	1	HEX	Link Status of Port 8
1512	0x5E8	32	ASCII	Description of Port 1
1544	0x608	32	ASCII	Description of Port 2
1576	0x628	32	ASCII	Description of Port 3
1608	0x648	32	ASCII	Description of Port 4
1640	0x668	32	ASCII	Description of Port 5
1672	0x688	32	ASCII	Description of Port 6
1704	0x6A8	32	ASCII	Description of Port 7
1736	0x6C8	32	ASCII	Description of Port 8
2024	0x7E8	2	HEX	Port 1 TX Packets
2026	0x7EA	2	HEX	Port 2 TX Packets
2028	0x7EC	2	HEX	Port 3 TX Packets

2030	0x7EE	2	HEX	Port 4 TX Packets
2032	0x7F0	2	HEX	Port 5 TX Packets
2034	0x7F2	2	HEX	Port 6 TX Packets
2036	0x7F4	2	HEX	Port 7 TX Packets
2038	0x7F6	2	HEX	Port 8 TX Packets
2088	0x828	2	HEX	Port 1 RX Packets
2090	0x82A	2	HEX	Port 2 RX Packets
2092	0x82C	2	HEX	Port 3 RX Packets
2094	0x82E	2	HEX	Port 4 RX Packets
2096	0x830	2	HEX	Port 5 RX Packets
2098	0x832	2	HEX	Port 6 RX Packets
2100	0x834	2	HEX	Port 7 RX Packets
2102	0x836	2	HEX	Port 8 RX Packets
2152	0x868	2	HEX	Port 1 TX Error Packets
2154	0x86A	2	HEX	Port 2 TX Error Packets
2156	0x86C	2	HEX	Port 3 TX Error Packets
2158	0x86E	2	HEX	Port 4 TX Error Packets
2160	0x870	2	HEX	Port 5 TX Error Packets
2162	0x872	2	HEX	Port 6 TX Error Packets
2164	0x874	2	HEX	Port 7 TX Error Packets
2166	0x876	2	HEX	Port 8 TX Error Packets
2216	0x8A8	2	HEX	Port 1 RX Error Packets
2218	0x8AA	2	HEX	Port 2 RX Error Packets
2220	0x8AC	2	HEX	Port 3 RX Error Packets
2222	0x8AE	2	HEX	Port 4 RX Error Packets
2224	0x8B0	2	HEX	Port 5 RX Error Packets
2226	0x8B2	2	HEX	Port 6 RX Error Packets
2228	0x8B4	2	HEX	Port 7 RX Error Packets
2230	0x8B6	2	HEX	Port 8 RX Error Packets
2280	0x8E8	1	HEX	Status of Spanning Tree

2.3.9 HTTPS

This subsection enables the users to set the HTTPS (HyperText Transfer Protocol Secure) for the web-based management user interface of the switch. This option will encrypt the normal HTTP message between the switch and the client PC to secure their communication over the network. To access the web GUI when this option is enabled, the users can also access the switch via https://10.0.50.1 for enchanced security during device configuration. Clicking on the **Update** button when you change the option to update it on the managed switch.

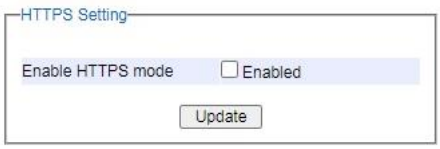

Figure 2.15 HTTPS Setting Webpage

2.4 Forwarding

There are many network technologies for forwarding packets over network. In this industrial managed switch, three main technologies are implemented: QoS, rate control, and storm control. Figure 2.16 depicts the submenus under the Forwarding section.

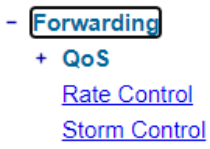

Figure 2.16 Forwarding Dropdown Menu

2.4.1 QoS

Quality of Service (QoS) is the ability to provide different priority to different applications, users, or data flows. QoS guarantees a certain level of performance to a data flow by using the following metrics: transmitted bit rate, bit error rate, delay, jitter, and probability of packet dropping. QoS guarantees are important if the network capacity is insufficient, especially for application that requires certain bit rate and is delay sensitive. For any network that is best effort, QoS cannot be guaranteed, except that resource is more than sufficient to serve users.

Controlling network traffic needs a set of rules to help classify different types of traffic and define how each of them should be treated as they are being transmitted. This managed switch can inspect both 802.1p Class of Service (CoS) tags and DiffServ tags called Differentiated Services Code Point (DSCP) to provide consistent classification.

In the QoS section, three QoS mechanisms are included: queuing methods or packet scheduling disciplines in **Setting** section, **CoS Queuing Mapping** section, and **DSCP Mapping** section, as shown in Figure 2.17. Table 2.8 summarizes the descriptions of QoS Setting. See notes in the following subsection for more details.

Figure 2.17 QoS Dropdown Menu

Table 2.8 Descriptions of QoS Setting

Label	Description	Factory Default

Setting	Queuing Methods (packet scheduling disciplines) includes **Strict Priority, Weighted Round-Robin,** and **Deficit Round Robin**. The detailed descriptions and comparison are given in the following subsection.	Strict Priority
CoS Queuing Mapping	**For 802.1p CoS only** which is a header mapping, switch only checks Layer 2 (L2) 802.1p CoS priority bits.	802.1p CoS
DSCP Mapping	**For DiffServ** which is a header mapping, switch checks DiffServ Code Point (DSCP).	802.1p DiffServ

2.4.1.1 QoS Setting

Two types of queuing methods are configurable in this managed switch: Strict Priority and Weighted Round-Robin.

In **Strict Priority**, the QoS scheduler allows the highest priority queue to preempt other queues as long as there are still packets waiting to be transmitted in the highest priority queue. This mode guarantees that traffic in the highest queue is always transmitted first. Only if the high priority queues are empty, the lower priority queues can be transmitted. Queue 0 (Q0) to Queue 7 (Q7) are ranked from the lowest priority queue to the highest priority queue. Therefore, packets in Q7 will be all transmitted first before packets in Q6, and packets in Q6 will all be sent first before packets in Q5, and so on in this order.

Weighted Round Robin (WRR) is the simplest approximation of generalized processor sharing (GPS). In WRR, each packet flow or connection has its own packet queue in a network interface controller. It ensures that all service classes have access to at least some configured amount of network bandwidth to avoid bandwidth starvation. But WRR has a limitation, as it is unfair with variable length packets. It only provides the correct percentage of bandwidth to each service class only if all of the packets in all the queues are the same size or when the mean packet size is known in advance. Usually, a weight of each queue is set proportion to requested bit rate. Each queue is served proportionally to its weight for a service cycle. Figure 2.18 depicts the QoS Setting webpage.

By default, the QoS in the managed switch works under the Strict Priority mode. For Weighted Round Robin, packet weights of Q0 to Q7 are set in term of packet as followings.

- COS Q0 = 2 packets
- COS Q1 = 1 packet
- COS Q2 = 3 packets
- COS Q3 = 6 packets
- COS Q4 = 2 packets
- COS Q5 = 17 packets
- COS Q6 = 25 packets
- COS Q7 = 33 packets

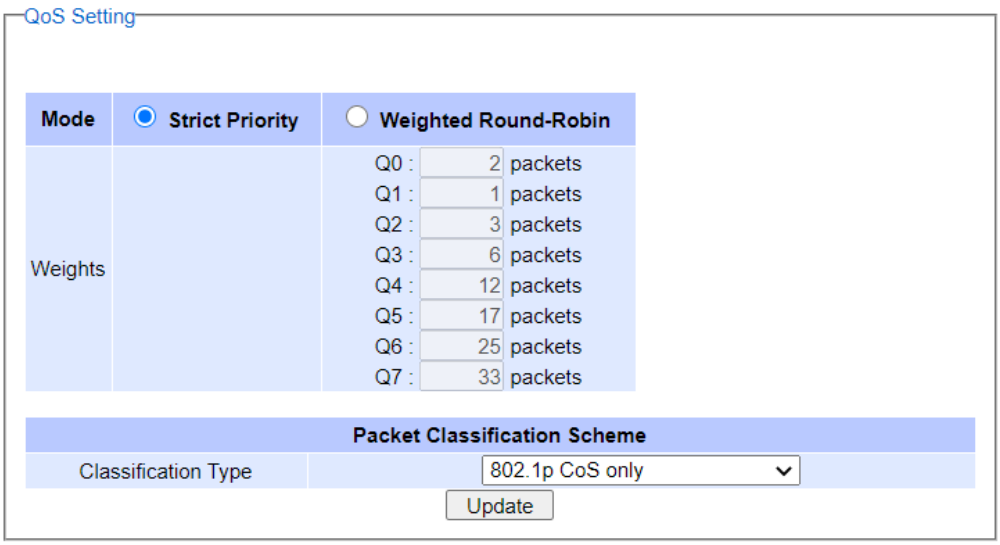

Figure 2.18 QoS Setting Webpage

At the bottom of the QoS Setting webpage in 錯誤! 找不到參照來源。, the users can select the packet classification scheme that will be used by the managed switch. There are two classification types to choose from the drop-down list: **802.1p CoS only** or **Both 802.1p CoS and DiffServ**. The default classification type is **802.1p CoS only**. Note that after changing the schedule discipline, setting the desired weights if any for the WRR or DWRR, or selecting the classification type, please click on the **Update** button to enable them on the switch.

2.4.1.2 CoS Queue Mapping

802.1p CoS is the QoS technique developed by the IEEE P802.1p working group, known as Class of Service (CoS) mechanism at Media Access Control (MAC) level. It is a 3-bit field called the priority code point (PCP) within an Ethernet frame header (Layer 2) when using VLAN tagged frames as defined by IEEE 802.1Q. It specifies a priority value between 0 and 7 that can be used by QoS to differentiate traffic. When this option is enabled, the switch inspects the 802.1p CoS tag in the MAC frame to determine the priority of each frame.

The switch can classify traffic based on a valid 802.1p (CoS - Class of Service) priority tag. These options allow users to map Priority Code Point (PC) within an Ethernet frame header to different CoS priority queues as shown in Figure 2.19. The user can choose the desired CoS Priority Queue from the drop-down list from Q1 to Q7 for each PCP value. Descriptions of priority queue in CoS Queue Mapping page are summarized in Table 2.9.

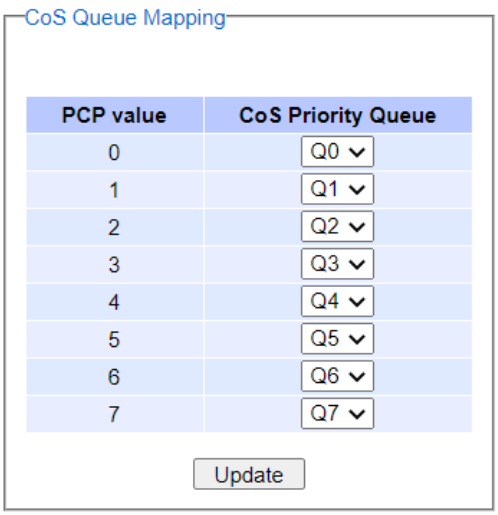

Figure 2.19 Mapping Table of CoS Webpage

Table 2.9 Priority queue descriptions

Label	Description	Factory Default
PCP	Priority Code Point within the Ethernet frame header. PCP 0 is the lowest priority and 7 is the highest priority.	PCP 0 -> Q0 PCP 1 -> Q1 PCP 2 -> Q2 PCP 3 -> Q3 PCP 4 -> Q4 PCP 5 -> Q5 PCP 6 -> Q6 PCP 7 -> Q7
CoS Priority Queue	The priority queue that a specific Ethernet frame needs to be assigned into.	

2.4.1.3 DSCP Mapping

DiffServ/ToS stands for Differentiated Services/Type of Services. It is a networking architecture that specifies a simple but scalable mechanism for classifying network traffic and providing QoS guarantees on networks. DiffServ uses a 6-bit Differentiated Service Code Point (DSCP) in the 8-bit differentiated services field (DS field) in the IP header for packet classification purposes. The DS field and ECN field replace the outdated IPv4 TOS field in IPv4 to make per-hop behavior decisions about packet classification and traffic conditioning functions, such as metering, marking, shaping, and policing.

The RFCs (Request for Comments) do not dictate the way to implement Per-Hop Behaviors (PHBs). Atop implements queuing techniques that can base their PHB on the IP precedence or DSCP value in the IP header of a packet. Based on DSCP or IP precedence, traffic can be put into a particular service class. Packets within a service class are treated the same way.

DiffServ allows compatibility with legacy routers, which only supports IP Precedence, since it uses the DiffServ Code Point (DSCP), which is the combination of IP precedence and Type of Service fields.

TOS (Type of Service) of the switch can be configured with the default queue weights as shown in Figure 2.20. Note that the TOS consists of DSCP (Differentiated Service Code Point (6 bits)) and ECN (Explicit Congestion Notification (2 bits)). The users can assign TOS values (**DSCP**) to predefined queue types (**Priority**) manually using DSCP Mapping web page in Figure 2.20. The priority number can be between 0 to 7 where the number 7 is the highest priority and 0 is the lowest priority. After assigning any new priority to a DSCP, please click the **Update** button at the bottom of the page to allow the new mapping to take effect.

DSCP Mapping

DSCP	Priority	DSCP	Priority	DSCP	Priority	DSCP	Priority
0x00(0)	0	0x01(1)	0	0x02(2)	0	0x03(3)	0
0x04(4)	0	0x05(5)	0	0x06(6)	0	0x07(7)	0
0x08(8)	1	0x09(9)	1	0x0A(10)	1	0x0B(11)	1
0x0C(12)	1	0x0D(13)	1	0x0E(14)	1	0x0F(15)	1
0x10(16)	2	0x11(17)	2	0x12(18)	2	0x13(19)	2
0x14(20)	2	0x15(21)	2	0x16(22)	2	0x17(23)	2
0x18(24)	3	0x19(25)	3	0x1A(26)	3	0x1B(27)	3
0x1C(28)	3	0x1D(29)	3	0x1E(30)	3	0x1F(31)	3
0x20(32)	4	0x21(33)	4	0x22(34)	4	0x23(35)	4
0x24(36)	4	0x25(37)	4	0x26(38)	4	0x27(39)	4
0x28(40)	5	0x29(41)	5	0x2A(42)	5	0x2B(43)	5
0x2C(44)	5	0x2D(45)	5	0x2E(46)	5	0x2F(47)	5
0x30(48)	6	0x31(49)	6	0x32(50)	6	0x33(51)	6
0x34(52)	6	0x35(53)	6	0x36(54)	6	0x37(55)	6
0x38(56)	7	0x39(57)	7	0x3A(58)	7	0x3B(59)	7
0x3C(60)	7	0x3D(61)	7	0x3E(62)	7	0x3F(63)	7

Update

Figure 2.20 Mapping Table of DSCP and ECN Webpage

2.5 SNMP

The SNMP (“Simple Network Management Protocol”) is used in network management systems to monitor the state of attached devices that require the attention of an administrator. SNMP is a component of the “internet protocol suite” defined by the IETF (“Internet Engineering Task Force”). It consists of a set of standards for network management, including an application layer protocol, a database schema and a set of data objects. SNMP provides management data in the form of variables on the managed systems, which describe the system configuration. These variables can be queried (and sometimes changed) by managing applications. An “SNMP community string” is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). The string is included in every packet transmitted between the SNMP manager and the SNMP agent. The “SNMP community” acts like a password and is used to define the security parameters of SNMP clients in an SNMP v1 and SNMP v2c environments. The default “SNMP community” is “public” for both SNMPv1 and SNMPv2c before SNMPv3 is enabled. Once SNMPv3 is enabled, the “Communities” of SNMPv1 and v2c have to be unique and cannot be shared.

ATOP industrial managed switch support SNMP and can be configured in this tab page as shown in Figure 2.22. The SNMP setting has four parts, which are:
• SNMP Agent
• SNMP V1/V2c Community setting
• Trap Setting
• SNMP V3 Auth. Setting

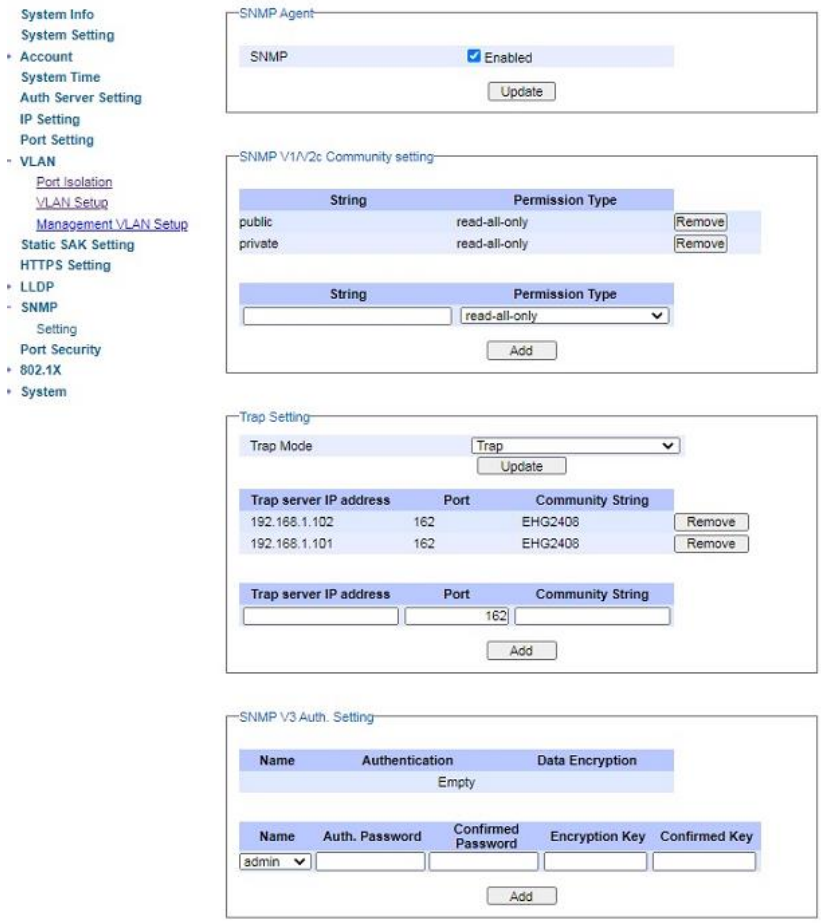

Figure 2.21 SNMP Settings Webpage

2.5.1 SNMP Agent

To enable SNMP agent on the managed switch, please check the **Enabled** box and click **Update** button as shown in Figure 2.17 **.** The SNMP version 1 (V1), version 2c (V2c) and version 3 are supported by Atop's managed switches. Basically, SNMP V1 and SNMP V2c have simple community string based authentication protocol for their security mechanism, while SNMP V3 is improved with cryptographic security**.**

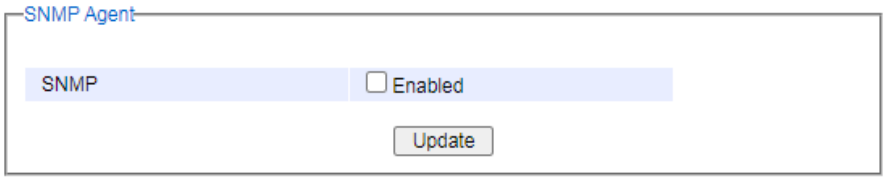

Figure 2.22 SNMP Enabling Box

Table 2.10 Descriptions of SNMP Setting

Label	Description	Factory Default
SNMP	Check the box to enable SNMP V1/V2c/V3.	Disabled

2.5.2 SNMP V1l V2c Community Setting

The managed switch supports SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string matching for authentication. This authentication will allow network management software to access the information or data objects defined by Management Information Bases (MIBs) on the managed switch. Note that this simple authentication is considered a weak security mechanism. It is recommended to use SNMP V3, if possible. There are two levels of authentications or permission type in EHG2408, which are read-all-only or read-write-all. For example, in our default setting as shown in Figure 2.18, an SNMP agent, which is a network management software module residing on the managed switch, can access all objects with read-all-only permissions using the string *public*. Another setting example is that the string *private* has permission of read-write-all.

This community string option allows the users to set a community string for authentication or remove existing community string from the list by clicking on the **Remove** button at the end of each community string item. The users can specify the string names on the **String** field and the type of permissions from the dropdown list as shown in Figure 2.18 briefly provides descriptions of SNMP's community string setting.

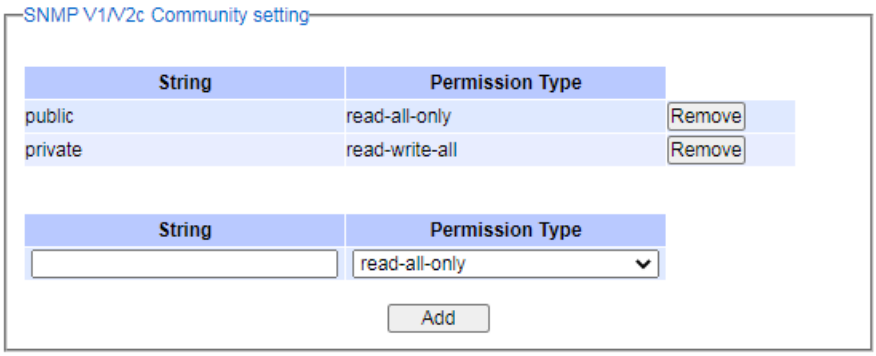

Figure 2.23 SNMP Community Strings

Table 2.11 Descriptions of Community String Settings

Label	Description	Factory Default
(Community) Strings	Define name of strings for authentication. Max. 15 Characters.	**Public** (read-all-only) **Private** (read-write-all)
Permission Type	Choose a type from the dropdown list: read-all-only and read-write-all. See notes below for a briefed explanation.	-

*NOTE:
Read-all-only: permission to read OID 1 Sub Tree.
Read-write-all: permission to read/write OID 1 Sub Tree.

2.5.3 Trap Setting

The managed switch provides a trap function that allows switch to send notification to agents with SNMP traps or inform. The notifications are based on the status changes of the switch such as link up, link down, warm start, and cold start. For inform mode, after sending SNMP inform requests, switch will resends inform request if it does not receive response within 10 seconds. The switch will try re-send three times. This option allows users to configure SNMP Trap Setting by setting the destination IP Address of the Trap server, Port Number of the Trap server, and Community String for authentication. Figure 2.19 shows these Tap Setting's options. The first line enables the users to select the Trap Mode which can be either **Trap** or **Inform**. Please click on the **Update** button after selecting the desired Trap Mode. After entering all required fields for Trap Setting in the last line, please click on the **Add** button. Table 2.10 summarizes the descriptions of trap receiver settings.

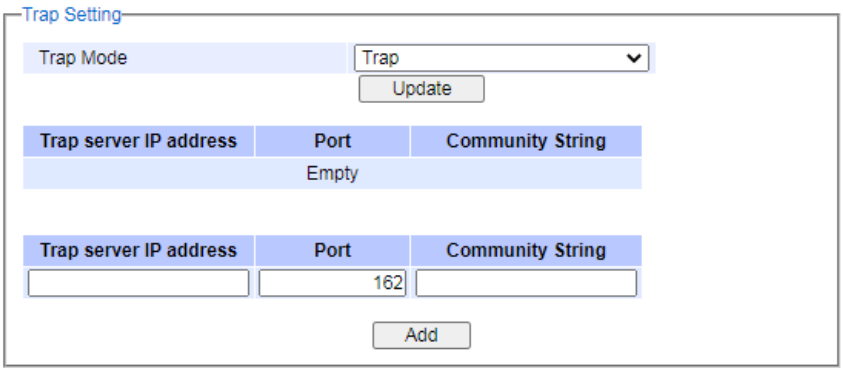

Figure 2.24 Example of Trap Receiver Setting

Table 2.12 Descriptions of Trap Receiver Settings

Label	Description	Factory Default
Trap Mode	Choose between Trap and Inform	Trap
Trap server IP address	Enter the IP address of your Trap Server.	NULL
Port	Enter the trap Server service port.	162
Community String	Enter the community string for authentication. Max. 15 characters.	NULL

2.5.4 SNMP V3 Auth. Setting

As mentioned earlier, SNMP V3 is a more secure SNMP protocol. In this part, the users will be able to set a password and an encryption key to enhance the data security. When choosing this option, the users can configure SNMP V3's authentication and encryption. MD5 (Message-Digest algorithm 5) is used for authentication password and DES (Data Encryption Standard) is used for data encryption algorithm. Figure 2.20 shows the SNMP V3 Authentication Setting' options. The users can view existing SNMP V3 users' setting on the upper table where it provides information about user name, authentication type, and data encryption. The users have an option to remove existing SNMP V3 user by clicking on the **Remove** button in the last column of each entry. To add a new SNMP V3 user, the users have to select the user **Name** from the dropdown list which can be either **Admin** or **User**. Then, the authentication password with a maximum length of 31 characters has to be entered in the **Auth. Password** field and re-entered again in the **Confirmed Password** field. Note that if no password is provided, there will be no authentication for SNMP V3. Finally, the encryption key with a maximum length of 31 characters can be entered in the **Encryption Key** and re-entered again in **Confirmed Key** field. After filling all the required fields, please click on **Add** button to update the information on the managed switch. Table 2.11 lists the descriptions of SNMP V3 settings.

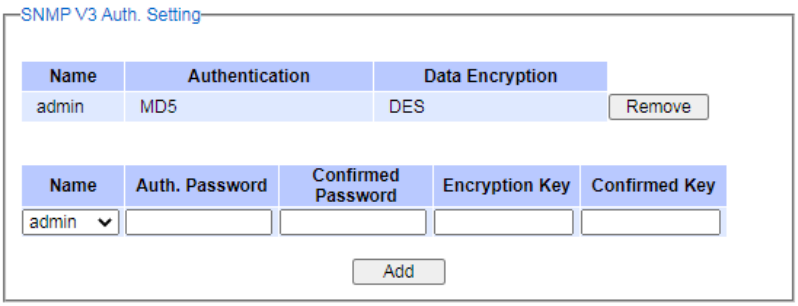

Figure 2.25 SNMPv3 Users' Options

Table 2.13 Descriptions of SNMP V3 Settings

Label	Description	Factory Default
Name	Choose from one of the following options: **Admin**: Administration level. **User**: Normal user level.	Admin
Auth. (Authentication) Password	Set an authentication password for the user name specified above. If the field is left blank, there will be no authentication. Note that the authentication password is based on MD5. Max. 31 characters.	NULL
Confirmed Password	Re-type the Authentication Password to confirm.	NULL
Encryption Key	Set encryption key for more secure protection of SNMP communication. Note that the encryption algorithm is based on DES. Max. 31 characters.	NULL
Confirmed Key	Re-type the Encryption Key	NULL

2.6 Spanning Tree

The RSTP (**R**apid **S**panning **T**ree **P**rotocol) can detect and stop network loops, as well as provide "Backup Links" between switches, bridges or routers. It allows a switch to interact with other RSTP-compliant switches in the network to ensure that only one path exists between any two stations on the network.
The switch supports RSTP as IEEE 802.1w Rapid Spanning Tree Protocol defined:
The switch uses IEEE 802.1w RSTP, which allows faster convergence of the "Spanning Tree". In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, there are longer delays because the device that causes a topology change first notifies the "Root Bridge" and then the network. RSTP remove unwanted learned addresses from the filtering database.
• In RSTP, the port states are Discarding, Learning and Forwarding.

STP Switch Port States
• **"Blocking"** If a port causes a "Switching Loop" (looping connection between two ports), user data can no longer be sent or received. However, the port can go into the "Forwarding" state if the other active connections fail and the "Spanning Tree" algorithm determines that the port may transition to that state. BPDU data is still received and sent in the "Blocking" state.
• **"Listening"** The switch processes BPDUs and waits for possible new information that would cause it to return to the "Blocking" state.
• **"Learning"** Even if the port does not yet forward any frames (packets), it can learn source addresses from frames received and add them to the filter database ("Switching Database").
• **"Forwarding"** The port is in normal operating mode and receives and sends data. STP still monitors incoming BPDUs that would indicate that the port should return to the "Blocking" state to prevent a loop.
• **"Disabled"** It is not strictly part of the STP because a network administrator can manually disable a port.

RSTP Bridge Port Roles

• **"Root"** The "Root Port" is a forwarding port that can best transmit data from the "Non-Root Bridge" to the "Root Bridge."
• **"Designated"** This is a forwarding port for every LAN segment.
• **"Alternate"** This port represents an alternate path to the "Root Bridge." However, the path is different than for the "Root Port."
• **"Backup"** This port is used as a backup/redundant path to a segment to which another "Bridge Port" is already connected.
• **"Disabled"** This is not actually part of STP because a network administrator can manually disable a port.

2.6.1 RSTP Setup

Functions of the RSTP

RSTP detects and breaks network loops provides backup links between switches, bridges or routers.

Default values: Forward Delay 15s, Mag Age 20s and Hello Time 2s.

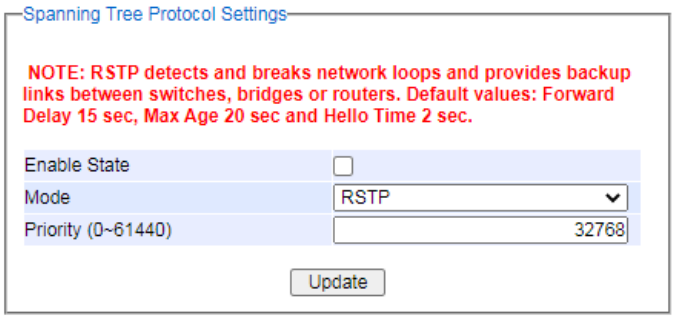

Figure 2.26 Spanning Tree Protocol Settings Webpage

Table 2.14 Descriptions of Spanning Tree Protocol Settings Webpage

Spanning Tree Protocol Settings			
Parameter	**Default**	**Description**	
Enable State			The "STP/RSTP" function is not enabled for the switch.
			The "STP/RSTP" function is enabled for the switch.
Bridge Parameters			
Parameter	**Default**	**Description**	
Priority (Range: 0~61440)	**32768**	In the input field, enter a value for the priority. The lower the numerical value you assign, the higher the priority of this bridge is. Valid range: 0 … 61440	

2.6.2 RSTP Port Setup

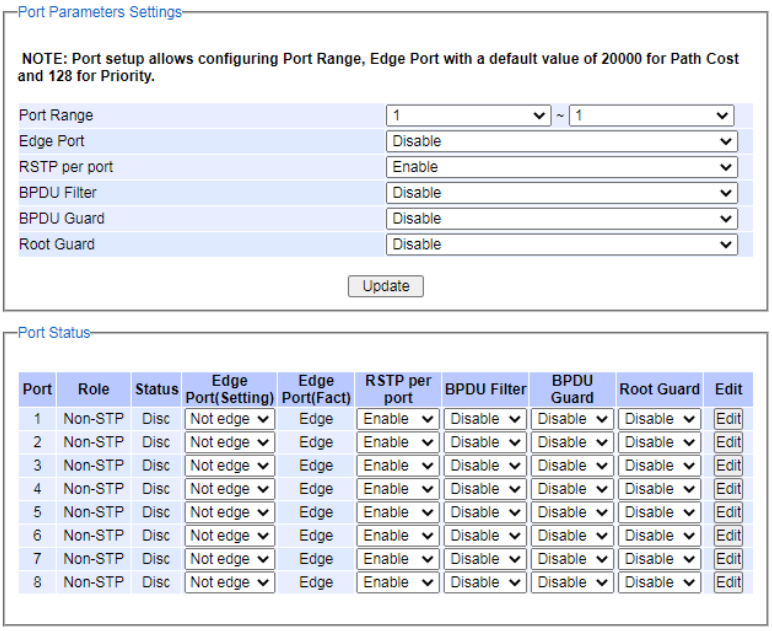

Figure 2.27 Spanning Tree Port Parameters Settings Webpage

Table 2.15 Descriptions of Spanning Tree Port Parameters Settings Webpage

Port ParameterSettings		
Parameter	**Default**	**Description**
PortRange	**1…8(16)**	Selecta portorportrangein theselection boxforwhich you wantto configure the “STP/RSTP” settings.
	1…8(16)	Selecta portorportrangein theselection boxforwhich you wantto configure the“STP/RSTP” settings.
EdgePort	**Disable**	Select“Disable” in the selection boxto disable the “EdgePort”porttypeforthespecificport.
	Enable	Select“Enable”in the selection boxtoenable the “EdgePort”porttypeforthespecificport.
BPDU Filter	**Disable**	Select“Disable”inthe selectionboxto disable the BPDU filter functionforthe specificport.
	Enable	Select“Enable”in the selection boxtoenable the BPDUfilter function for thespecificport.
BPDU Guard	**Disable**	Select“Disable”inthe selectionboxto disable the “BPDUGuard”functionforthespecificport.
	Enable	Select“Enable”in the selection boxtoenable the “BPDUGuard”functionforthespecificport.
ROOT Guard	**Disable**	Select“Disable”inthe selectionboxto disable the “ROOTGuard”functionforthespecificport.
	Enable	Select“Enable”in the selection boxto enablethe“ROOTGuard”functionforthespecificport.
PortStatus		
Parameter	**Default**	**Description**
Port	1…8(16)	Thiscolumn showstheportnumbers.
Role	AlternatedDesignatedRootBackupNone	Thiscolumn displaystheroleoftheport.
Status	DiscardingBlockingListeningLearningForwardingDisabled	Thiscolumn displaystheportstatus.

EdgePort	DisableEnable	Thiscolumn displaysthestatusofthe“EdgePort”function.
BPDU Filter	DisableEnable	Thiscolumn displaysthestatusoftheBPDUfilterfunction.
BPDU Guard	DisableEnable	Thiscolumn displaysthestatusofthe“BPDUGuard”function.
ROOT Guard	DisableEnable	Thiscolumn displaysthestatusofthe“RootGuard”function.
Edit		Preselection forediting.

2.7 VLAN

2.7.1 Port Isolation

Port isolation is a port-based virtual LAN feature. It partitions the switching ports into virtual private domains designated on a per port basis. Data switching outside of the switch’s private domain is not allowed. The VLAN tag information of the packets is ignored.
This feature is a per-port setting to configure the egress port(s) for the specific port to forward its received packets. If the CPU port (port 0) is not an egress port for a specific port, the host connected to the specific port cannot manage the switch.
If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. CPU refers to the switch’s management port. By default, it forms a VLAN with all ETHERNET ports. If it does not form a VLAN with a specific port, then the switch cannot be managed from that port.

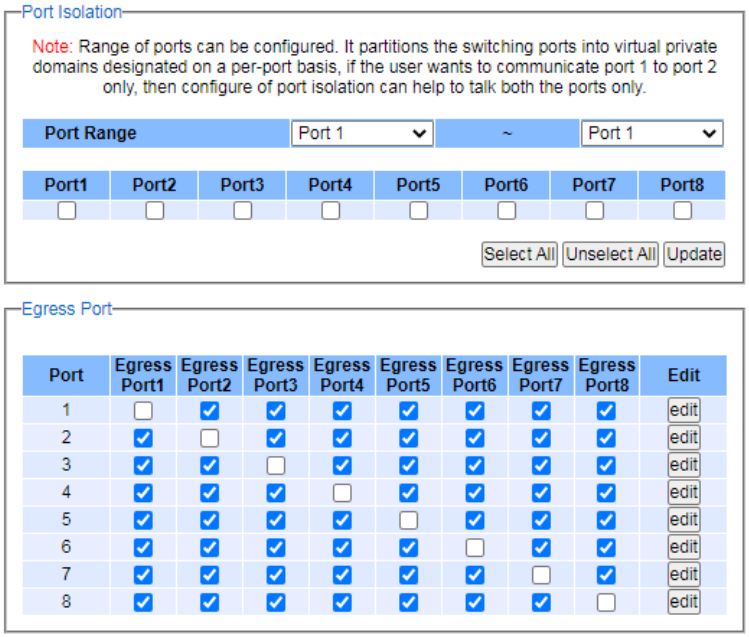

Figure 2.28 Port Isolation Webpage

Table 2.16 Descriptions of Port Isolation

Port Isolation Settings				
Parameter		**Default**	**Description**	
Port Range		1 … 8 (16)	Select a port or port range in the selection box for which you want to configure the "Port Isolation" setting.	
		1 … 8 (16)	Select a port or port range in the selection box for which you want to configure the "Port Isolation" setting.	
Egress Port			An egress port is an outgoing port through which a data packet leaves. Selecting a port as an egress port means it will communicate with the port currently being configured.	
	Select All	☐	☐	No egress port is selected.
			☑	All egress ports are selected.
	Disable All	☐	☐	No egress port is disabled.
			☑	All egress ports are disabled.
	☐ 0 (CPU) … ☐ 8	☐	☐	The egress port is not enabled.
			☑	The egress port is enabled.
Port Isolation Status				
Parameter		**Default**	**Description**	
Port		V	V	"V" indicates that the port's packets can be sent to this port.
Egress Port			-	"-" indicates the port's packets cannot be sent to this port.
Edit			Preselection for editing.	

2.7.2 VLAN Setup

A VLAN ("Virtual LAN") is a group of hosts with a common set of requirements that communicate as if they were attached to a broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Networks can be reconfigured through software instead of spatially separated devices.
VID ("VLAN-ID") is the identification of a VLAN that is generally used by the IEEE 802.1Q standard. It has 12 bits and allows the identification of 4096 (212) VLANs. Of the 4096 possible VIDs, VID 0 is used to identify "Priority Frames", and value 4095 (FFF) is reserved, so the maximum possible number of VLAN configurations is 4094. But the Lean Managed Switch has 5 VLANs available.
A "Tagged VLAN" uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across "Bridges" – they are not confined to the switch on which they were created. VLANs can be created statically (manually by users) or dynamically via the GVRP ("GARP VLAN Registration Protocol"). The VLAN ID associates a frame with a specific VLAN and provides the information that switches need in order to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID ("Tag Protocol Identifier", residing within the type/length field of the "ETHERNET Frame") and two bytes of TCI ("Tag Control Information", which starts after the source address field of the "ETHERNET Frame").
The CFI ("Canonical Format Indicator") is a single-bit flag, always set to zero for ETHERNET switches. If a frame received at an ETHERNET port has a CFI of 1, the frame should not be output to an untagged port. The remaining 12 bits define the VLAN ID, giving a possible maximum number of 4096 VLANs. Note that the user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant, and the default VID of the ingress port is used as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify "Priority Frames", and value 4095 (FFF) is reserved, so the maximum possible number of VLAN configurations is 4094.

TPID	User Priority	CFI	VLAN ID
2 bytes	3 bits	1 bit	12 bits

Forwarded Tagged and Untagged Frames
Each port on the switch is capable of forwarding tagged and untagged frames. When a frame is forwarded from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the switch first decides where to forward the frame and then strips off the VLAN tag. When a frame is forwarded from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the switch first decides where to forward the frame and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is "VLAN 1" for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

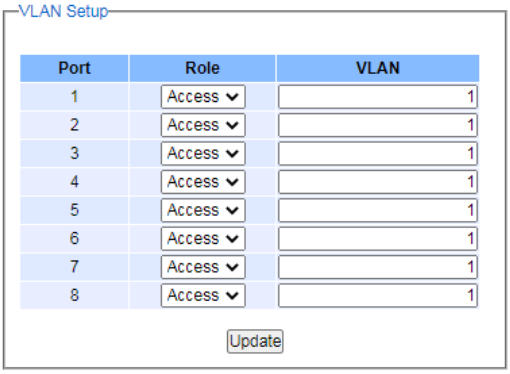

Figure 2.29 VLAN Setup Webpage

Table 2.17 Descriptions of VLAN Setup Webpage

VLAN Setup		
Parameter	**Default**	**Description**
Port	**Access**	Select "Access" in the selection box to access the port.
	Trunk	Select "Trunk" in the selection box to trunk the port.
VLAN		In the input field, select a VLAN ID from 1 zo 4094.

2.7.3 Management VLAN Setup

Here the management VLAN Identification number (ID) is configured based on the IEEE 802.1Q standard. The default value is VID = 1. Note that the ID can be the number from 1 to 4094. If the users change the management VLAN ID to other number, please click the **Update** button to set it on the managed switch. Figure 2.25 depicts the Management VLAN Setup Webpage and Table 2.16 describes the Management VLAN Setup.

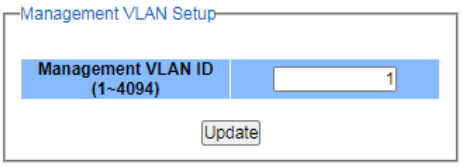

Figure 2.30 Management VLAN Setup Webpage

Table 2.18 Descriptions of Management VLAN Setup

Label	Description	Factory Default
Management VLAN ID	Configure the management VLAN ID that can be accessed this switch. Range from 1 to 4094.	1

2.8 Security

2.8.1 Port Security

The switch receives the MAC address of a device that is connected to a specific port direction and allows data forwarding. The functions of the switch allow control over which and how many devices may be connected to a switch port. The "Port Security" functions can specify the maximum number of MAC addresses per interface. If this number is exceeded, incoming packets with new MAC addresses are dropped. A MAC address table can be

used to check this. The static MAC addresses are included for this limit. Figure 2.26 shows the webpage fir port security settings.

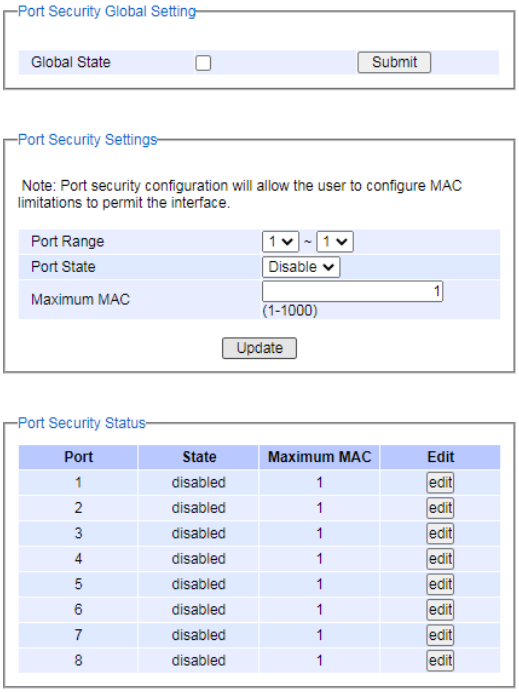

Figure 2.31 Port Security Webpage

Table 2.19 Descriptions of Port Security

Label	Description	Factory Default
Port Security Global Settings		
Global State	Enable/Disable port security feature	Uncheck
Port Security Settings		
Port Range	Select a port or port range in the selection box for which you want to configure the port security setting	1~1
Port State	Enable/Disable port security for a port or port range	Disable
Maximum MAC	User can enter maximum number of MAC addresses per interface	1
Port Security Status		
Port	This column shows the port numbers	1~8
State	This field indicates whether port security is enabled or disabled	disabled
Maximum MAC	This column displays the maximum number of MAC addressed	1
Edit	Preselection for editing	edit

2.8.2 802.1X

802.1X is an IEEE standard for port-based Network-Access Control. It provides an authentication mechanism to devices that want to attach to a LAN or WLAN. This protocol restricts unauthorized clients from connecting to a LAN through ports that are opened to the Internet. The authentication basically involves three parties (see Figure 2.27): a supplicant, an authenticator, and an authentication server.

- Supplicant: A client device that requests access to the LAN.

- Authentication Server: This server performs the actual authentication. We utilize RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) as the authentication server.
- Authenticator: The Authenticator is a network device (i.e. the EHG2408 Managed Switch) that acts as a proxy between the supplicant and the authentication server. It passes around information, verifies information with the server, and relays responses to the supplicant.

The authenticator acts like a security guard to a protected network. The supplicant is not allowed accessing to the protected side of the network through the authenticator until the supplicant's identity has been validated and authorized. With 802.1X authentication, a supplicant and an authenticator exchange **EAP** (**E**xtensible **A**uthentication **P**rotocol, an authentication framework widely used by IEEE). Then the authenticator forwards this information to the authentication server for verification. If the authentication server confirms the request, the supplicant (client device) will be allowed to access resources located on the protected side of the network.

RADIUS: The RADIUS is a networking protocol that provides authentication, authorization and accounting (AAA) management for devices to connect and use a network service. Figure 2.27 shows a diagram of RADIUS authentication sequence.

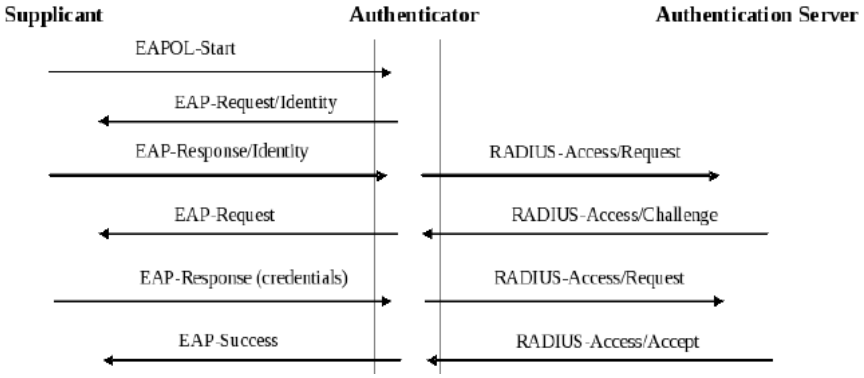

Figure 2.32 RADIUS Authentication Sequence

The **802.1X** option under the Security section is subdivided into three sub-menus which are: **Setting**, **Parameters Setting**, and **Port Setting**.

2.8.2.1 Setting

The 802.1X security mechanism can be enabled in this webpage as shown in Figure 2.33. When the users check the Enabled box, the rest of the option fields will become active. The users then have to enter all the required fields to configure the 802.1X Setting which are the IP address of RADIUS server, the RADIUS server's port number, RADIUS server's accounting port number, NAS identifier, shared key and confirmed shared key. Additionally, the Forward 802.1x option can also be enabled in the last field. Summary of 802.1X Setting options are given in Table 2.20. After changing all the required fields, please click on the **Update** button.

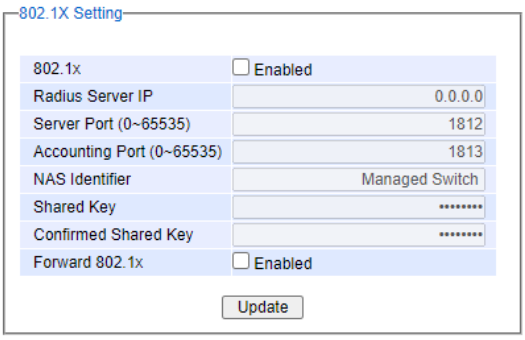

Figure 2.33 802.1X Setting Webpage

Table 2.20 Descriptions of 802.1X Setting

Label	Description	Factory Default
802.1x	Choose whether to enable 802.1X for all ports or not	Disabled
Radius Server IP	Set RADIUS server IP address	0.0.0.0
Server Port	Set RADIUS server port number. The range is 0 ~ 65535.	1812
Accounting Port	Set the accounting port number of the RADIUS server. The range is 0 ~ 65535.	1813
NAS Identifier	Specify the identifier string for 802.1X Network Access Server (NAS).Max. Of 30 characters.	Managed Switch
Shared Key	A shared key between the managed switch and the RADIUS Server. Both ends must be configured to use the same key. Max. Of 30 characters.	NULL
Confirm Shared Key	Re-type the shared key string.	Dependent
Forward 802.1x	Choose whether to enable forwarding of 802.1x	Disable

2.8.2.2 Parameters Setting

There are a number of 802.1X parameters that the users might want to fine tune. This can be done on this webpage as shown in Figure 2.29. These parameters are related to the authentication periods or timeout durations and maximum number of authentication requests. Table 2.21 summarizes the descriptions of these parameters and their default setting. Please clicking on the Update button after the users changed any of the parameters.

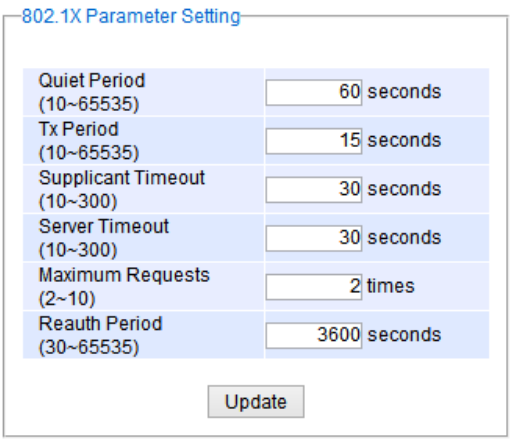

Figure 2.34 802.1X's Parameters Setting Webpage

Table 2.21 Descriptions of 802.1X Parameters

Label	Description	Factory Default
Quiet Period	Waiting time between requests when the authorization has failed. Range from 10 to 65535 seconds.	60
Tx Period	Waiting time for the supplicant's EAP response packet before retransmitting another EAP request packet. Range from 10 to 65535 seconds.	15
Supplicant Timeout	Waiting time for the supplicant to response to the authentication server's EAP packet. Range from 10 to 300 seconds.	30
Server Timeout	Waiting time for the authentication server to response to the supplicant's EAP packet. Range from 10 to 300 seconds.	30
Maximum Requests	Maximum number of the retransmissions that the authentication server sends EAP request to the supplicant before the authentication session times out. Range from 2 to 10 seconds.	2
Reauth Period	Time between periodic re-authentication of the supplicant. Range from 30 to 65535 seconds.	3600

2.8.2.3 Port Setting

The user can individually configure 802.1x security mechanism on each port of the EHG7XXX managed switch as shown in Figure 2.30. Each port can be set for any of the four authorization modes which are Force Authorization, Force Unauthorization, IEEE 802.1X Standard Authorization, and no authorization (N/A) as described in Table 2.48. The lower part of the webpage is a table display the current status of authorization mode and state of each port on the managed switch. To enable the 802.1X security on any of the port(s), click one of the port or press **Ctrl** key and click multiple ports on the list and choose the Authorization **Mode** from the pulldown list and click the **Update** button. To check the latest status of the 802.1X port setting, please click on the **Refresh** button.

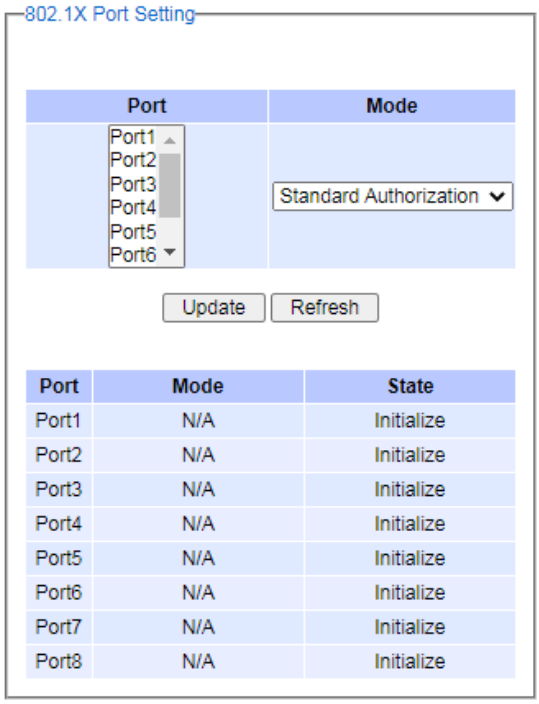

Figure 2.35 802.1x Port Setting Webpage

Table 2.22 Descriptions of 802.1X Port Setting

Label	Description	Factory Default
Port	Set specific ports to be configured.	Option
Mode	Choices: **Force Unauthorized:** Specify forced unauthorized **Force Authorized:** Specify forced authorized **Standard Authorization:** Specify authorization based on IEEE 802.1X **N/A**: Specify disable authorization	N/A

2.8.3 ACL

Access Control List (ACL) is the mechanism for network access control. The users configure the switch's filtering rules for accepting or rejecting some packets.
The numbers of matching rules can be at most 32. However, the main important rules that are mostly exercise are follows. Rules for filtering includes Source MAC address and Source IP address. When filtering is enabled, the matching rules are used to check whether the receiving packet is matched. If it is match, the packet will be rejected; otherwise it will be accepted. Note here that the matching rules later will be referred to as the entries of ACL.

The ACL webpage is depicted in Figure 2.31. To differentiate between each ACL entry, Index number from 1 to 32 is used. The ACL entry that has higher priority will be checked first before the lower priority. The Name field is for setting name of this rule.

Table 2.23 describes definition of each in details. Here note that if any field is empty, that ACL entry will be ignored.

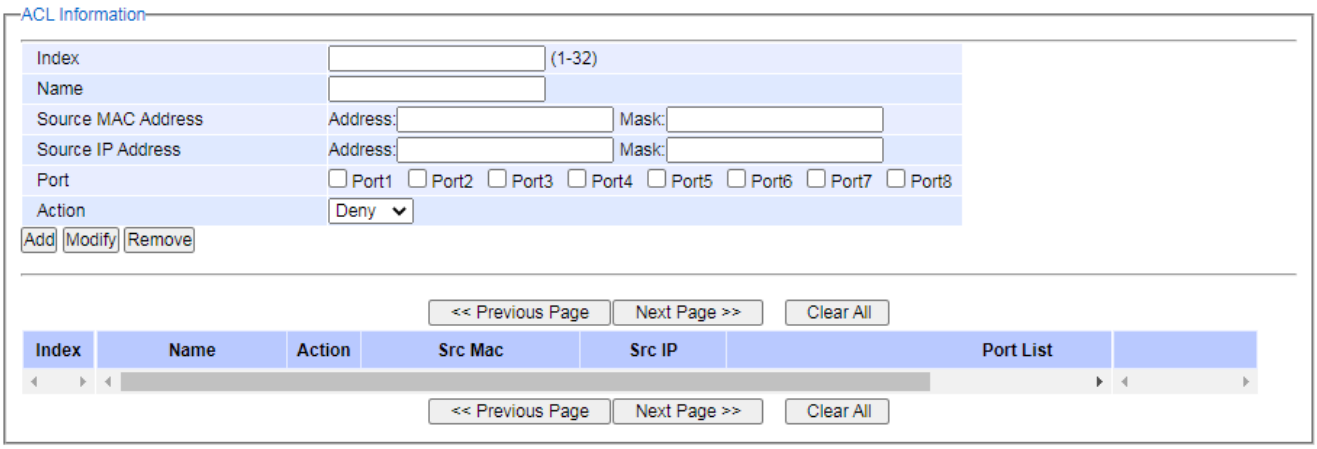

Figure 2.36 Security Access Control List Information Webpage

Table 2.23 Descriptions of ACL Entries for in ACL Webpage

ACL Entry	Definition	Range
Index	ACL priority	Priority (1-32)
Name	ACL rule name	Max length 32
Source MAC Address	MAC address are the fields of the Ethernet frame header. The Mask item is a bit mask for comparing range.	For every non-zero bits in the Mask, its relative bit in the IP address will be compared. If the Mask is 0.0.0.0.0.0, then this condition is always accepted. If the Mask is empty, it is considered equal to the Mask of FF:FF:FF:FF:FF:FF and all of bits in the IP Address are compared.
Source IP Address	IP Addresses are the fields of the IPv4 header. The Mask item is a bit mask for comparing range.	For every non-zero bits in the Mask, its relative bit in the IP address will be compared. If the Mask is 0.0.0.0, then this condition is always accepted. If the Mask is empty, it is considered equal to the Mask of 255.255.255.255 and all of bits in the IP Address are compared.
Port	DUT's port number	1~8
Action	Configure rule to Deny or Permit	Deny / Permit

2.9 LLDP

Link **L**ayer **D**iscovery **P**rotocol (**LLDP**) is an IEEE802.1ab standard OSI layer-2 protocol. LLDP allows Ethernet network devices to advertise details about themselves, such as device configuration, capabilities and identification. The advertise packets are periodically sent to directly connected devices on the network that are also using LLDP or so called its neighbors. LLDP is a "one hop" unidirectional protocol in an advertising mode.

LLDP information can only be sent to and received by devices, no solicit information or state changes between nodes. The device has a choice to turn on and off sending and receiving function independently. Advertised information is not forward on to other devices on the network. LLDP is designed to be managed with SNMP. Applications that use this protocol include topology discovery, inventory management, emergency services, VLAN assignment, and inline power supply.

Link Layer Discovery Protocol (LLDP) section consists of **LLDP Setting** and **LLDP Neighbors** as shown in Figure 2.32.

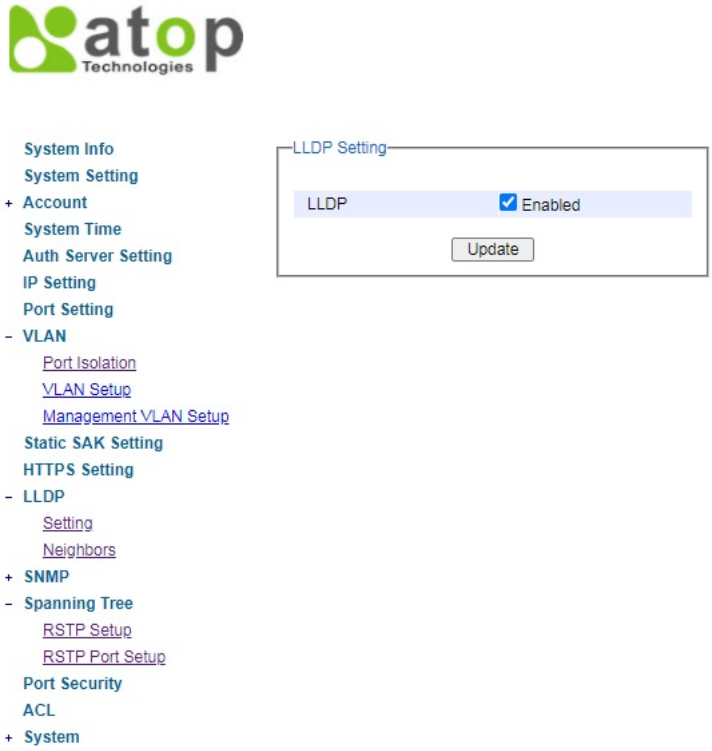

Figure 2.37 LLDP Dropdown Menu

2.9.1 Setting

In Figure 2.33, the LLDP Setting webpage allows users to have options for enabling or disabling the LLDP, as well as setting LLDP transmission parameters. This LLDP function should be enabled if users want to use Atop's Device Management Utility (formerly called Device View) to monitor the switches' topology of all LLDP devices in the network.

Figure 2.38 LLDP Setting Webpage

2.9.2 Neighbors

This menu allows the user to view the LLDP's neighbor information of the managed switch as shown in Figure 2.34. The Neighbor Information table contains Chassis ID, Port ID, Port Description, Device Name, Device Description and Management Address on each Port of the managed switch.

An example of neighbor information table is depicted in Figure 2.35. Note that this example is based on a display format EHG75XX managed switch in which System Name is changed to Device Name and System Description is changed to Device Description in the latest version of EHG2408's firmware.

LLDP Neighbors

Port	Neighbor Information					
	Chassis ID	Port ID	Port Description	Device Name	Device Description	Management Address
Port1						
Port2						
Port3						
Port4						
Port5						
Port6						
Port7						
Port8						

Figure 2.39 LLDP Neighbors Webpage

LLDP Neighbors

Port	Neighbor Information					
	Chassis ID	Port ID	Port Description	Device Name	Device Description	Management Address
Port1						
Port2						
Port3						
Port4						
Port5						
Port6						
Port7						
Port8	00-60-E9-20-BE-27	port-008	Port 8	EHG7512-1	Managed Switch	http://10.0.50.11

Figure 2.40 Example of LLDP Neighbors Webpage

Table 2.24 Descriptions of LLDP Neighbors Webpage

Label	Description
Port	Indicates particular port number of the switch.
Chassis ID	Indicates the identity of the neighbor of this particular port.
Port ID	Indicates the port number of this neighbor.
Port Description	Shows a textual description of the neighbor port.
Device Name	Indicates the device name/ hostname of the neighbor.
Device Description	Shows a more detailed description of the neighbor's device.
Management Address	Indicates neighbor's management IP address.

2.9 Fiber Speed

Port Setting webpage is shown in EHG2408-2SFP only as Figure 2.36. The users can control the speed of each fiber port modify speed and click "Update" button.

Port Setting

Port	Mode	Speed
Port7	Fiber	1000
Port8	Fiber	1000

Update

Figure 2.41 Port Setting Webpage

2.10 Port Setting

Port Control Setting webpage is shown in Figure 2.37. The users can control the state of each port by checking on the corresponding **Enable** box.

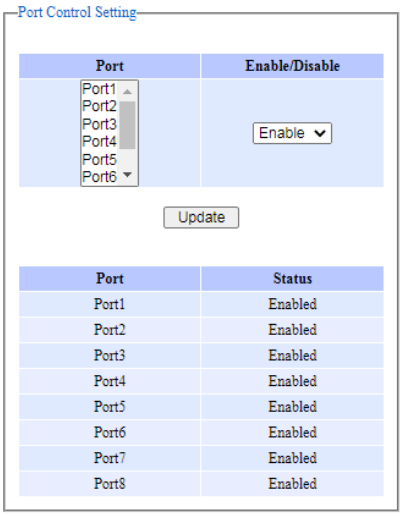

Figure 2.42 Port Setting Webpage

2.11 Static SAK Setting

EHG2408 series support advanced security features that allow traffic encryption and high throughput. MACsec or Media Access Control Security is a security standard specified by IEEE also called IEEE 802.1AE. This IEEE MAC security standard provides connectionless user data confidentiality, frame data integrity, and data origin authenticity. MACsec can establish point-to-point security on Ethernet links between directly connected nodes. ATOP's secure smart switches support this security feature and can be used to transparently secure an IEEE 802 LAN connection to a peer device (such as another switch) that also supports the MACsec.

MACsec defines two terms called secure channel and connectivity association when setting up a secure communication between two switches. A secure channel in MACsec is unidirectional and used for transmitting (outbound traffic) or receiving (inbound traffic) data. A connectivity association when MACsec is enabled consists of two secure channels: one for inbound traffic and one for outbound traffic.

The point-to-point links can be secured by MACsec after matching security keys are exchanged and verified between the ports on two different secure switches. There are two modes for setting up the static security keys: Secure Association Key (SAK) and Connectivity Association Key (CAK). Note that EHG2408 only supports SAK mode.

Static Association Key (SAK):
The static secure association key (SAK) security mode is when the user manually configured the same static secure association key (SAK) on both sides of a connection. There is no key server in this mode and the key must be matched on the ports of both switches. This can be viewed as setting up two secure channels within a connectivity association. It is suggested to have a periodic manual key update in order to prevent the key to be broken by brute-force attack.

Static secure association key (SAK) setting webpage is shown in Figure 2.38. To enable secure association mode on secure MACsec switch's port(s), first select **one or multiple ports** from the list under the Ports. Then, check the **Enabled** box. Then, enter the **Secure Channel Identifier (SCI)** with a 16-digit hexadecimal number (i.e., 0,1,2,…,a,b,c,d,e,f) and enter the **Secure Association Key (SAK)** with a 32-digit hexadecimal number. Finally, click on the **Add/Modify** button to add the setting to the table below like Figure 2.39.

The selected port(s) will use the given static **SAK** as the secure key to secure all the traffic. If any two switches have the same SCI and SAK, they can securely communicate. If there is any non-secured traffic that uses incorrect SCI and SAK, the traffic will be dropped by the ingress port of the switch. The description of the static SAK setting fields are summarized in Table 2.24.

To disable the SAK setting for any of the port(s), simply select the desired port(s) from the list and uncheck the Enabled box. Then click on the **Add/Modify** button. This will update the status of the setting in the table below.

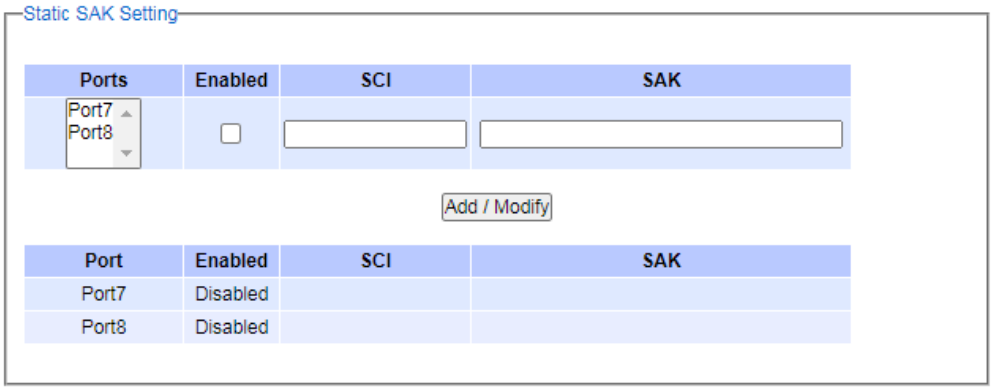

Figure 2.43 Static SAK Setting Webpage

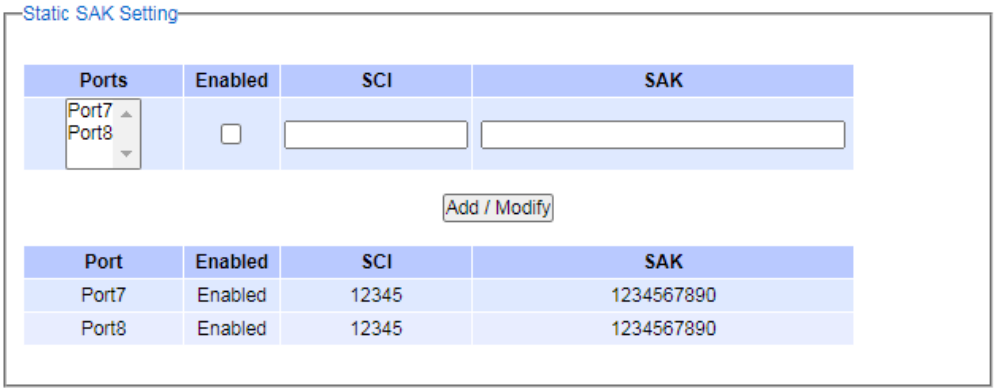

Figure 2.44 Static SAK Setting Example

Table 2.25 Descriptions of Static SAK Setting Webpage

Label	Description	Factory Default
Port	Set specific ports to be configured.	Option
Enabled	Check the box to enable static secure association key (SAK) mode for the selected port(s)	Unchecked
SCI	Secure Channel Identifier (SCI) is a 16-digit hexadecimal number. Note that if the user did not configure all digits of SCI, all remaining digits will be auto-configured to 0s.	Null
SAK	Secure Association Key (SAK) is a 32-digit hexadecimal number. Note that if the user did not configure all digits of SAK, all remaining digits will be auto-configured to 0s.	Null

2.12 System

2.12.1 System Log

The submenus under the System Log are: **Setting** and **Log**.

2.12.1.1 Settings

Figure 2.45 shows System Log related settings configuration. The actual recorded log event will be shown in Event Log on the next subsection. Here the users can enable how the log will be saved and/or delivered to other system. The log can be saved to flash memory inside the managed switch and/or it can be sent to a remote log server. The users need to select the log level and provide the IP address of a remote log server and the service log service port. Please click on the Update button after finishing the setup. Table 2.26 describes the details of parameters setting for the system log.

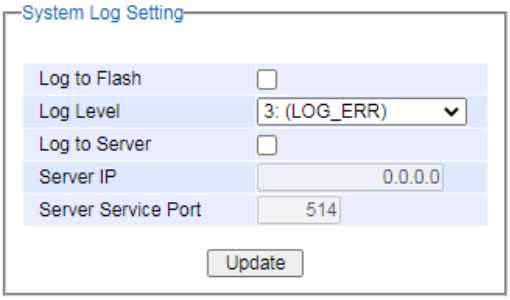

Figure 2.45 System Log Setting Webpage

Table 2.26 Descriptions of System Log Settings

Label	Description	Factory Default
Log to Flash	**Checked**: Saving log event into flash memory. The flash memory can keep the log event files even if the switch is rebooted. **Unchecked**: Saving log event into RAM memory. The RAM memory cannot keep the log event files after each reboot.	Uncheck
Log Level	Set the log level to determine what events to be displayed on the next webpage (**Log**). The level selection is inclusive. For example, if 3 :(Log_ERR) is selected, all 0, 1, 2 and 3 log levels will be implied. Range from Log 0 to Log 7.	3: (LOG_ERR)
Enable Log to Server	**Checked**: Enable Syslog Server. **Uncheck**: Disable Syslog Server. If enabled, all recorded log events will be sent to the remote System Log server.	Uncheck
Server IP	Set the IP address of Syslog server	0.0.0.0
Server Service Port	Set the service port number of System Log server. Range from Port 1 to Port 65535.	514

2.12.1.2 Log

Figure 2.41 shows an example of all of the event's logs. Note that they are sorted by date and time. Table 2.27 provides explanation of each column and the button's functions on the System Log webpage.

System Log

Index	Date	Time	Up Time	Level	Event
1/13	2017.01.03	12:46:21	00d19h17m00s	ERR	lighttpd[469]: admin(10.0.50.100):Authentication Success from web
2/13	2017.01.02	17:52:19	00d00h22m57s	ALERT	syslog: Link Status: Port1 link is up
3/13	2017.01.02	17:52:16	00d00h22m54s	ALERT	syslog: Link Status: Port1 link is down
4/13	2017.01.02	17:52:03	00d00h22m41s	ALERT	syslog: Link Status: Port1 link is up
5/13	2017.01.02	17:52:00	00d00h22m38s	ALERT	syslog: Link Status: Port1 link is down
6/13	2017.01.02	17:51:57	00d00h22m35s	ALERT	syslog: Link Status: Port1 link is up
7/13	2017.01.02	17:51:54	00d00h22m32s	ALERT	syslog: Link Status: Port1 link is down
8/13	2017.01.02	17:33:18	00d00h03m56s	ERR	lighttpd[469]: admin(10.0.50.100):Authentication Success from web
9/13	2017.01.02	17:31:23	00d00h02m01s	ALERT	syslog: Link Status: Port1 link is up
10/13	2017.01.02	17:31:20	00d00h01m58s	ALERT	syslog: Link Status: Port1 link is down
11/13	2017.01.02	17:29:40	00d00h00m18s	ALERT	syslog: Link Status: Port1 link is up
12/13	2017.01.02	17:29:35	00d00h00m13s	ALERT	syslog: System warning config. changed
13/13	2017.01.02	17:29:35	00d00h00m13s	ALERT	syslog: TZ was changed

<< Previous Page Next Page >>

Show All Clear All Download

Figure 2.46 Event Log Webpage

Table 2.27 Descriptions of Event Log

Label	Description
Index	Indicate the index of a particular log event
Date	Indicate the system date of the occurred event
Time	Indicate the time stamp that this event occurred
Up Time	Indicate how long the system (managed switch) has been up since this event occurred.
Level	Indicate the level of this event.
Event	Details description of this event.
Previous Page	Display events on the previous page.
Next Page	Display events on the next page
Show All	Click to display all events.
Clear All	Click to clear all events
Download	Download or save the event log to the local computer

2.12.2 Warning/ Alarm

The warning/alarm section consists of three subsections: **Setting**, **SMTP Setting**, and **Log**.

2.12.2.1 Settings

There are two different types of Warning or Alarm: Link Status Alarms and System Log Alarms as shown in Figure 2.47. The Link Status Alarms are related to the activities of particular port(s). System Log Alarms are related to the overall functionalities of the switch. This webpage allows the users to configure how each type of the alarm events will be sent alarm mail to users. After finish configuring the alarms, please click the **Update** button.

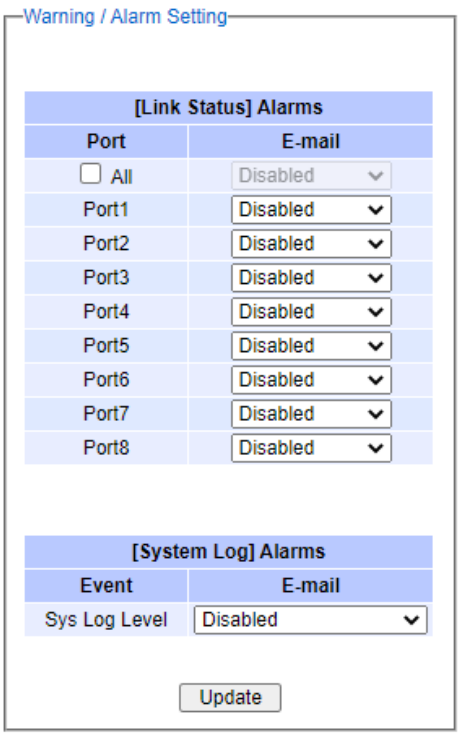

Figure 2.47 Webpage of Warning Event Selection

In Link Status Alarms, DUT can send notifications via **E-mail** in case if Link is UP, Link is Down, or Link is UP/DOWN. Table 2.28 summarizes the link status alarm event selection. Note the users can enable the alarm events for all ports simultaneously by checking the box in front of the **All** entries.

Table 2.28 Descriptions of Link Status Alarm Event Selection

Label	Description	Factory Default
Port	Indicates each port number.	-
Port state event	**Disabled:** Disables alarm function, i.e. no alarm message will be sent. **Link Up:** Alarm message will be sent when this port/link is up and connection begins. **Link Down:** Alarm message will be sent when this port/link is down and disconnected. **Link Up /Down:** Alarm message will be sent whenever there's a change, i.e. connection begins or connection disrupted.	Disabled

In System Log Alarms, the users also can send notifications via **E-mail.** Table 2.29 describes the System Log Level which can be selected for the System Log Alarm event notification.

Table 2.29 Descriptions of System Log Alarm Event Selection

Label	Description	Factory Default
System log event	Disable: Disable power status detection. 0: (**LOG_EMERG**): Enable log level 0~7 detection.	Disabled

	1: **(LOG_ALERT):** Enable log level 1~7 detection. 2: **(LOG_CRIT):** Enable log level 2~7 detection. 3: **(LOG_ERR):** Enable log level 3~7 detection. 4: **(LOG_WARNING):** Enable log level 4~7 detection. 5: **(LOG_NOTICE):** Enable log level 5~7 detection. 6: **(LOG_INFO):** Enable log level 6~7 detection. 7: **(LOG_DEBUG):** Enable log level 7 detection. See note below for specific log level description.	

***NOTE:** - **Log levels** are inclusive. In other words, when log level is set to 0, an alarm is triggered whenever 0, 1, 2… 6, and/or 7 happens. When log level is set to 5, an alarm is triggered whenever 5, 6, and/or 7 happens.

0: Emergency: system is unstable
1: Alert: action must be taken immediately
2: Critical: critical conditions
3: Error: error conditions
4: Warning: warning condition
5: Notice: normal but significant condition
6: Informational: informational messages
7: Debug: debug-level messages

2.12.2.2 SMTP Settings

Simple **M**ail **T**ransfer **P**rotocol (**SMTP**) is an internet standard for email transmission across IP networks. In case any warning events occur as configured in Section 2.12.1.1, the system can send an alarm message to users by e-mail. Here, the users will be allowed to modify E-mail-related settings for sending the system alarms (Link Status and System Log), as shown in Figure 2.48.

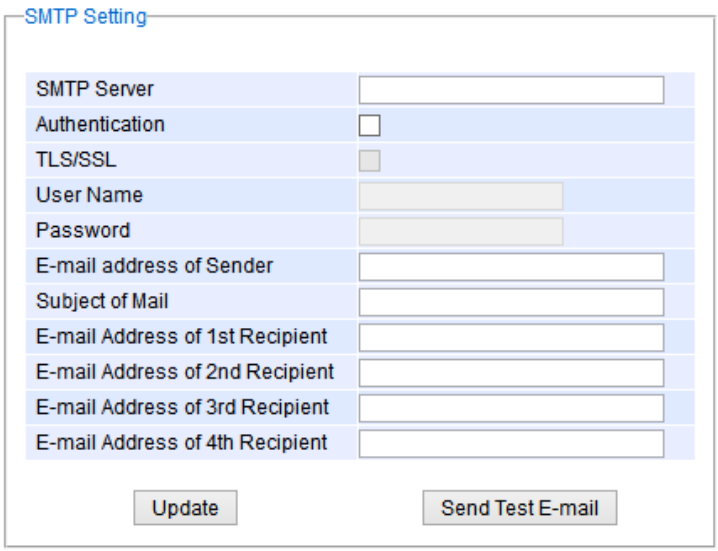

Figure 2.48 SMTP Setting Webpage

An example of SMTP Setting is shown in Figure 2.49. After entering all the necessary fields, please click on the Update button to allow the setting to take effect. Note that the users can try to send a Test E-mail according the SMTP setting on this webpage by clicking on the **Send Test E-mail** button. The description of each SMTP Setting parameter is summarized in Table 2.30.

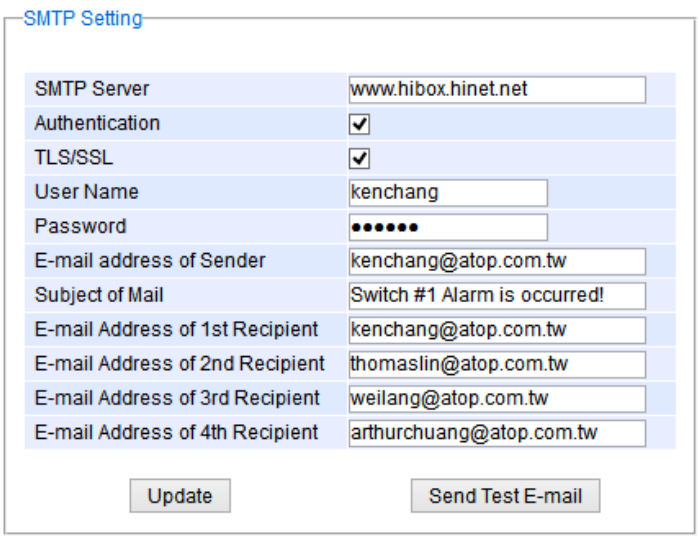

Figure 2.49 Example of SMTP Setting

Table 2.30 Descriptions of SMTP Setting

Label	Description	Factory Default
SMTP Server	Configure the IP address of an out-going e-mail server	NULL
Authentication	Enable or disable authentication login by checking on the box. If enabled, SMTP server will require authentication to login. Thus, the users will also need to setup User Name and Password to connect to the SMTP server	Disable (Unchecked)
TLS/SSL	Enable or disable Transport Layer Security (TLS) or Secure Sockets Layer (SSL) which is an encryption mechanism for communication with the SMTP Server	Disable (Unchecked)
Username	Set the user name (or account name) to login. Max. 31 char.	NULL
Password	Set the account password for login. Max. 15 characters.	NULL
E-mail Address of Sender	Configure the sender e-mail address	NULL
Mail Subject	Type the subject of this warning message. Max. 31 characters.	NULL
E-mail Address of 1st Recipient	Set the first receiver's E-mail address.	NULL
E-mail Address of 2nd Recipient	Set the second receiver's E-mail address.	NULL
E-mail Address of 3rd Recipient	Set the third receiver's E-mail address.	NULL
E-mail Address of 4th Recipient	Set the fourth receiver's E-mail address.	NULL
Update	Update these modifications on the managed switch	-
Send Test E-mail	Send a test email to recipient(s) above to check accuracy.	-

2.12.2.3 Log

Managed switches warns its users in case any event occurs. A table called Warning/Alarm Log in this section displays the warning events as shown in Figure 2.50 Warning/Alarm Log Webpage. At the top of the table, the users can click on the **Clear Log** to remove all entries in the **Warning/Alarm Log** table. To obtain the latest event on the able, the users have to click on the **Refresh** button.

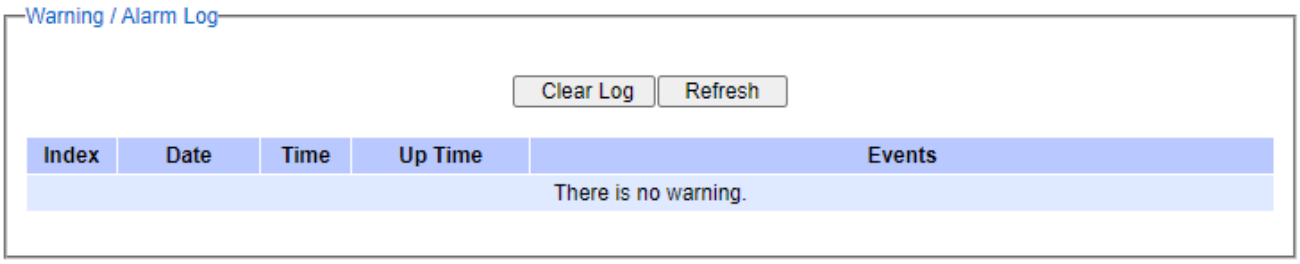

Figure 2.50 Warning/Alarm Log Webpage

Table 2.31 Descriptions of Warning / Alarm Log

Label	Description
Clear Log	Clears all warning events that are displayed.
Refresh	Obtain the latest Warning / Alarm events
Index	Display the index of the Warning/Alarm events as an entry number over a total number of events
Date	The date that the alarm/event occurred.
Time	The time that the alarm/event occurred.
Up Time	The duration of time since the start up time of the switch until the alarm/event occurred.
Events	Description of the alarm events

2.12.3 Backup / Restore

In **Backup/Restore Config** function, the current configuration of the EHG2408 switch can be downloaded to a local computer and saved it as a backup. Additionally, the users can restore a previously backup configuration from a local computer to the EHG2408 switch. It will replace the current configuration.

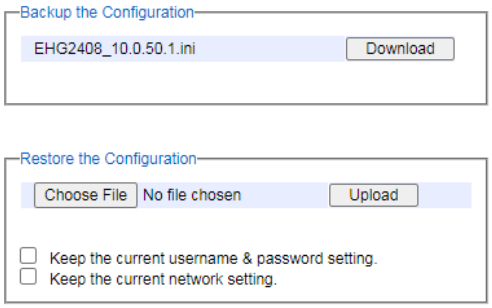

Figure 2.51Figure 2.51 shows the webpage for Backup/Restore the configuration via HTTP. It is divided into two parts: **Backup the Configuration** and **Restore the Configuration**. When clicking on the **Download** button on the upper part of the page (**Backup the Configuration**), the users will be prompt to **Opening** the file name "EHG2408_10.0.50.1.ini" by an application or to **Save File** to a destination. Choosing to Save File will back up the switch's current configuration to your local drive on the local computer.

To restore a configuration file to the switch, please move down to the **Restore the Configuration** part, then click the **Browse...** button to choose a configuration file from the local drive. Before clicking the **Upload** button, the users can check any of the options below the upload file which are to **Keep the current username & password setting** and to **Key the current network setting**. This will help prevent the users from the necessity to logging-in using a previously stored username, password or network configuration after settings are restored.

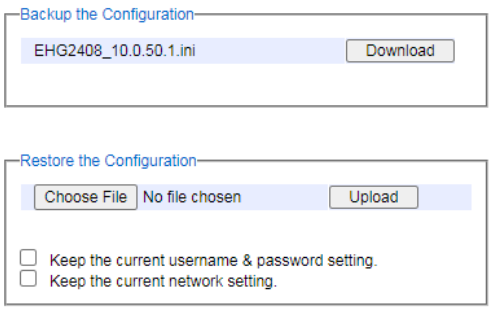

Figure 2.51 Backup/Restore Configuration via HTTP

2.12.4 Firmware Update

The users can update the device firmware via web interface as shown in Figure 2.52. To update the firmware, the users can download a new firmware from Atop's website and save it in a local computer. Then, the users can click "**Choose File"** button and choose the firmware file that is already downloaded. The switch's firmware typically has a ".dld" extension such as EHG2408-K317.dld. After that, the users can click **Update** button and wait for the update process to be done.

Note: please make sure that the switch is plug-in all the time during the firmware upgrade.

Figure 2.52 Firmware Update Webpage

2.12.5 Reset to Default

When the managed switch is not working properly, the users can reset it back to the original factory default settings by clicking on the **Reset** button as shown in Figure 2.53

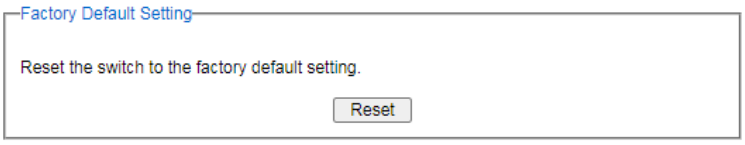

Figure 2.53 Factory Default Setting Webpage

2.12.6 Auto Default

EHG2408 series also provide alternative method for factory default setting as Figure 2.54. This feature can be achieved by setting up a Trivial File Transfer Protocol (TFTP) server. Note that the user need to install a TFTP application such as tftpd64 (https://bitbucket.org/phjounin/tftp64) on the PC that will be used to configure the switch. This TFTP server must be available and connected on the same local area network (LAN) as the EHG2408 switch, i.e. the PC that is installed this tftpd64 must be on the same LAN as the EHG2408. The EHG2408 will use a default IP address of 192.168.195.252 as a TFTP client while the TFTP Server will use a default IP address of 192.168.195.253. Note that default TFTP Address and its related parameters are summarized in Table 2.26.

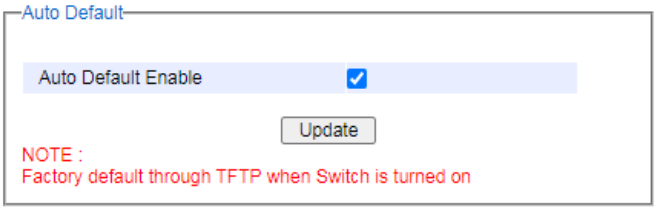

Figure 2.54 Factory Default Setting Webpage

Table 2.32 Default TFTP's Parameters

Model Name	Default TFTP		
	IP	Netmask	Gateway
EHG2408	192.168.195.252	255.255.255.0	192.168.195.254
EHG2408-2SFP	192.168.195.252	255.255.255.0	192.168.195.254

To perform automatic factory default setting, please follow these steps:

1. On the industrial smart secure switch, using the IP Setting menu as described in Section 0 to change the IP Address of the switch to 192.168.195.252 and set the Subnet Mask to 255.255.255.0. Note you will need to re-login to the switch via the web browser by entering the password after the changes.

2. On the PC with Windows Operating System, set the new IPv4 address for Ethernet Interface as 192.168.195.253 and Subnet Mask as 255.255.255.0 by going to the Internet Protocol Version 4 (TCP/IPv4) Properties. Note on Windows 10 OS, please select Settings → Network & Internet → Ethernet → Change adapter options. On previous version of Windows OS, go to Control Panel → Network and Internet → Network Connections. Then select the Ethernet icon as depicted in and right click on it and then select the Properties. A new window for Ethernet Properties will pop-up as shown in Figure 2.46. Next select **Internet Protocol Version 4 (TCP/IPv4)** from the list of items. Then click on the **Properties** button to bring up another pop-up window as shown in Figure 2.47. Fill in the information as shown in Figure 2.48. Note that you will also need to temporary disable the Windows Defender Firewall (or any other firewall software on the PC) to allow the tftp connection between the PC and the EHG2408 switch. Alternatively, you may allow only the TFTP Server apps to communicate through Windows Firewall. On Windows 10, you can disable the firewall by going through Settings → Windows Security → Firewall & network protection.

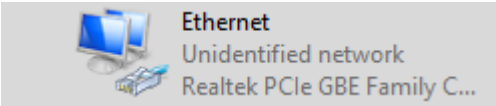

Figure 2.55 Ethernet Icon

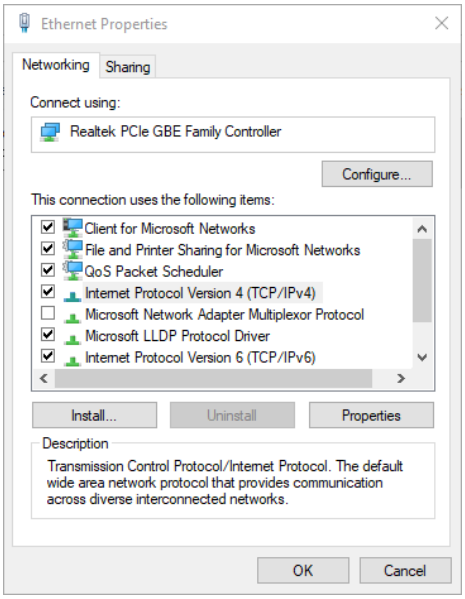

Figure 2.56 Ethernet Properties

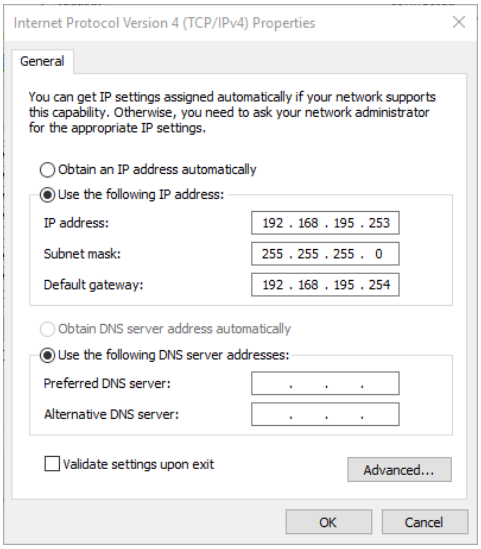

Figure 2.57 Internet Protocol Version 4 (TCP/IPv4) Properties

3. Open the TFTP Server (such as tftpd64) as shown in Figure 2.49 and set the Current Directory to C:\ or any directory of your choice.

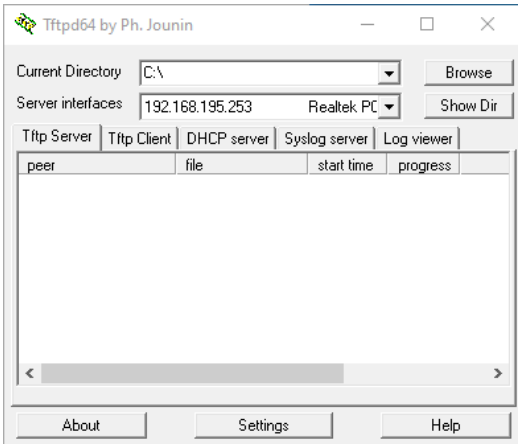

Figure 2.58 Tftpd64 Main Window

4. Create a text file using any text editor (such as notepad) and name it as “testerase.txt”. Then enter the MAC address of the EHG2408 device in the text file as shown in Figure 2.50. Note that you can find the MAC address of the device on the label on the case.

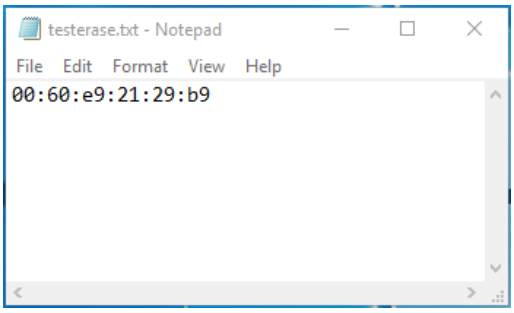

Figure 2.59 testerase.txt file

5. Save the text file under the C:\ directory or any directory of your choice.
6. Reboot the EHG2408 device by going to the Reboot System menu as described in Section 0 and the EHG2408 will execute the factory default setting. Note that the TFTP window will indicate the TFTP’s progress as shown in Figure 2.60.

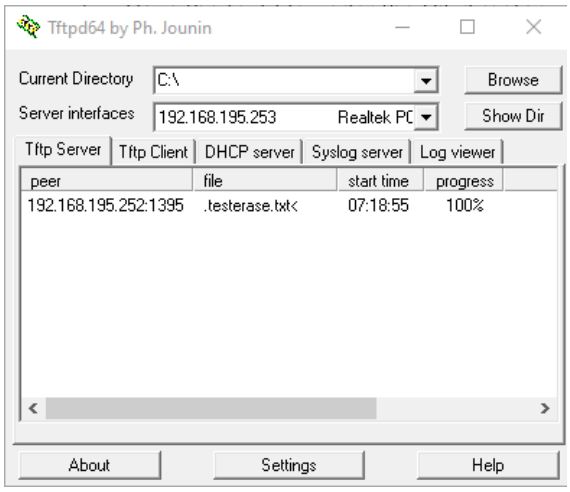

Figure 2.60 TFTP’s progress during the factory default setting

7. After the EHG2408 is rebooted, it will be reset back to its original factory default settings. Note that the default IP address of EHG2408 will be restored to 10.0.50.1. Therefore, you will need to change the PC’s IP address back to an address in the same subnetwork such as 10.0.50.100 in order to use the web browser

to login to the EHG2408 again. Moreover, it is recommended that you turn the Windows firewall back on to ensure the security of your PC after finishing the factory default setting.

2.12.7 Periodically Backup

Figure 2.61 shows the setting configuration of Periodic backup. Enabled this feature, users can auto backup configuration periodically and upload the backup configuration to the TFTP Server. Table 2.29 describes the setting parameters of Periodically Backup in details.

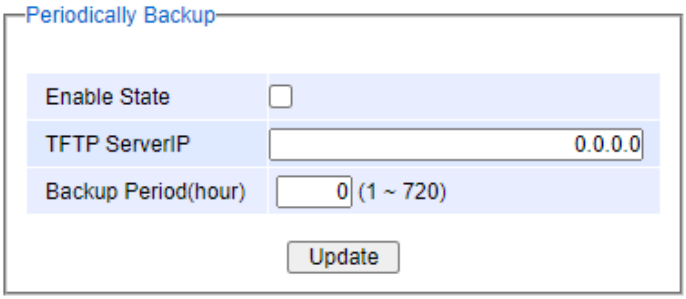

Figure 2.61 Periodic Backup Webpage

Table 2.33 Default TFTP's Parameters

Label	Description	Factory Default
Enable State	Enable/Disable periodic feature.	UnCheck
TFTP ServerIP	The TFTP Server IP address for periodic backup file upload.	0.0.0.0
Backup period(hour)	Configure the backup configuration file period.	0

2.12.8 Reboot System

An easy reboot function is provided in this webpage requiring only one single click on the **Reboot** button as shown in Figure 2.62.

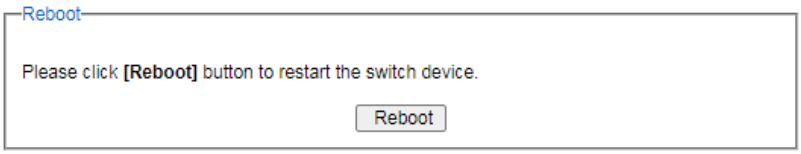

Figure 2.62 Reboot Webpage

2.12.9 Logout

A logout function is provided in this webpage requiring only one single click on the **Logout** button as shown in Figure 2.63.

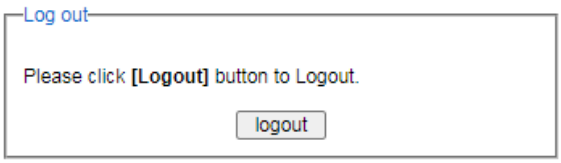

Figure 2.63 Logout Webpage

3 Configuring with Telnet

An alternative configuration method is the Telnet method and it is described in this chapter.

3.1 Telnet

Telnet is a remote terminal software to login to any remote telnet servers. It is typically installed in most of the operating systems. In order to use it, users open a command line terminal (e.g., cmd.exe for Windows Operating System). Note that only users with administrator (admin) access right as configured can use telnet to login to the device.

3.2 Telnet Log-in

After the command line terminal is opened, type in "telnet 10.0.50.1" as shown in Figure 3.1. Note that telnet command needs to follow by IP address or domain name. In this example, the default IP address is 10.0.50.1. If users change the switch IP address, the IP address to log-in should be changed to match the new switch IP address.

Figure 3.1 Telnet Command

Below are telnet login description :
Username：admin
Password：default
Mode of Operation: Three Mod of Operation
1. Privilege-Unprivileged Mode
2. Privilege Mode
3. Configuration Mode

- "disable" command is used to return or default privilege-unprivileged mode
- "enable" command is used to enters into privilege mode and password is "admin"
- "configure" command is used to enters the setting configuration mode

3.3 Command Line for Telnet

This chapter introduce EHG2408 command line descripton for Telnet. When users do not know the commands to use for the command line configuration, users can type in "?" and the commands are displayed.

Features Implemented List:

No	Feature	Settings	Show Command
1	Port Settings	Yes	Yes
2	Vlan Setup	Yes	Yes
3	Port Isolation	Yes	Yes
4	Management Vlan Setup	Yes	Yes
5	802.1x Setting	Yes	Yes
6	802.1x Parameter Settings	Yes	Yes
7	802.1x Port Settings	Yes	Yes

8	LLDP	Yes	Yes
9	SNTP	Yes	Yes
10	SNMP Setting	Yes	Yes
11	Network Settings	Yes	Yes
12	Port Mirror	Yes	Yes
13	ACL	Yes	Yes
14	Static SAK Settings	Yes	Yes
15	RSTP	Yes	Yes
16	Modbus Settings	Yes	No
17	Systeminfo	No	Yes
18	Default Reset	Yes	No
19	System Reboot	Yes	No

3.3.1 Port Mirror CLI commands:

Node	Command	Description
Configure	# mirror-settings enable sourcePort 3 destPort 2	This command used to enable the "Port Mirroring" on the switch with source port and mirror destination port.
Configure	# mirror-settings disable	This command used to disable the mirror (Optional source port and destination port)
Show	# show mirror-status ---------- Port Mirror ---------- Port Mirror : Enabled Mode : BOTH_RxTx Source_Port : 3 Destination_port : 2 ----------	This command displays the current "Port Mirroring" configurations.

3.3.2 Modbus Settings CLI commands:

Node	Command	Description
Configure	# modbus globalEnable	This command is used to set enable or disable the modbus
Configure	# modbus portValue 502	This command is used to set the modbus desire port number in the range of 1~65535.
Configure	# modbus address 33	This command is used to set modbus slave address
Show	# show modbusSettings Modbus Global State :Disabled Modbus Address :33 Modbus Port Number :502	This command displays the current Modbus Setting in the device

3.3.3 Port Setting CLI commands:

Node	Command	Description
Configure	# port-settings 3 enable	This command is used to enable the port with port number
Configure	# port-settings 3 disable	This command is used to disable the port with port number
Show	# show port-settings Port | State	This command displays the current port configurations.

	----------+---------- 1 Enabled 2 Enabled 3 Enabled 4 Enabled 5 Enabled 6 Enabled 7 Enabled 8 Enabled	

3.3.4 Device Network Setting CLI commands:

Node	Command	Description
Configure Ip Settings	# ip staticIP address 10.0.50.1 netMask 255.255.0.0 gateway 10.0.50 .254 primaryDNS 10.0.50.10	This command is used to set the device network ip address. Note: gateway and primaryDNS is optional parameter.
Configure dhcp	# ip dhcp enable	This command is used to enable or disable the dhcp feature in the device
Show	# show ip ---------- IP Setting ---------- DHCP : Disabled Static IP Address : 10.0.50.1 Subnet Mask : 255.255.0.0 Gateway : 10.0.50.254 Primary DNS : 10.0.50.10	This command used to view the current device network ip address configuration.

3.3.5 LLDP Setting CLI commands:

Node	Command	Description
Configure	# lldp-globalActive enable	This command is used to enable or disable the LLDP for active global.
Show Active State	# show lldp_activeState LLDP Global State : enabled	This command used to show the active state LLDP
Show Neighbor	# show lldp_neighbor 1 LLDP Global State : Enabled ------- IIdp -> 1 ------ Port ID : 8C:16:45:C3:2B:2B Chassis ID : 8C-16-45-C3-2B-2B System Name : System Description: Management Address:	This command is used to view the LLDP Neighbor information passing with port number

3.3.6 Port Security Setting CLI commands:

Node	Command	Description
Configure	# port-security globalActive enable	This command is used set Global enable/disable the port security feature.
Configure	# port-security settings 8 enable 1000 # port-security Settings 5 disable	This command used to set and enable/disable the individual port security functionality with desire MAC count 1 to 1000

Show	show port-security Port Security Global State:Enabled ---------- | Port | State | Maximum Mac ---------- 1 Disabled 1 2 Disabled 1 3 Disabled 1 4 Disabled 1 5 Disabled 1 6 Disabled 1 7 Disabled 1 8 Enabled 1000	This command used to view the current port security list of the device

3.3.7 Vlan Setting CLI commands:

Node	Command	Description
Configure	# vlan-add access 4 6 # vlan-add trunk 7 1,2,4,6,7	This command is used to configure the port Vlan id & access role
Show	#show vlan-portBased Port | Role | VLAN ID ----------+---------- 1 Access 1 2 Access 1 3 Access 1 4 Access 1 5 Access 1 6 Access 1 7 Trunk 1,2,4,6,7 8 Access 1	This command is used to view the current setting of Vlan configuration.
configure	# port-isolation 3 egrs1 1 egrs2 2 egrs3 4 egrs6 7 egrs8 8	This command is used to set the source port isolation list of destination port. Example: Source Port : 3 Destination Port : 1 2 4 7 8
Show	# show port-isolation FW | Egress | Port | Port-1 Port-2 Port-3 Port-4 Port-5 Port-6 Port-7 Port-8 ----------+---------- * 1 - V V V V V V V * 2 V - V V V V V V * 3 V V - V - - V V * 4 V V V - V V V V * 5 V V V V - V V V * 6 V V V V V - V V * 7 V V V V V V - V * 8 V V V V V V V -	This command is used to view the list of port isolation in the device.

3.3.8 802.1x Setting CLI commands:

Node	Command	Description
Configure	# 802.1X-settings enable 10.0.50.120 3456 567 Switch wago	This command is used set 802.1x Setting Example: Active Set = enable Radius Server IP : 10.0.50.120 Server Port : 3456 Account Port: 567

		NAS Identified: Switch Shared Key: wago Confirmed Key: wago
Show	#show 802.1X-settings ---------- 802.1X Settings ---------- 802.1x : Enabled Radius Server IP : 10.0.50.120 Server Port (0~65535) : 3456 Accounting Port (0~65535) : 567 NAS Identifier : Switch Shared Key : wago	This command is used to view the current setting of 802.1x settings
Configure	# 802.1X-parameter 120 20 100 40 5 3700	This command is used to set the 802.1x parameter setting: Example: Quiet Period: 120 Tx Period : 20 Supplication Timeout: 100 Server Timeout:40 Maximum Request : 5 Reauth Period : 3700
Show	# show 802.1X-parameter ---------- 802.1X Parameter Settings ---------- Quiet Period(10~65535 : 120 Tx Period(10~65535) : 20 Supplicant Timeout (10~300): 100 Server Timeout (10~300) : 40 Maximum Requests (2~10) : 5 Reauth Period (30~65535) : 3700	This command is use to view the 802.1X parameter settings.
Configure	# 802.1X-portSettings 3 std-auth	This command is used to configure 802.1x port authentication mode with respect to the port number. Example: Source Port: 3 Mode: std-auth (na std-auth force-unAuth force-auth)
Show	# show 802.1X-portSettings +---------- 802.1X Port Settings ---------- ------+ | Port | Mode | State | +---------- + N/A Initialize N/A Initialize Standard Authorization Initialize N/A Initialize N/A Initialize N/A Initialize N/A Initialize N/A Initialize	This command is used to view the 802.1x port settings mode list.

3.3.9 ACL Setting CLI commands:

Node	Command	Description
Configure	# acl-settings 4 wagoacl4 whitelist other 00:00:00:00:00:06 00:00:00:00:00:07 other 10.0.50.120 255.255.0.0 4	This command is used to configure the acl setting as example follows: Index :4 Profile Name: wagoacl4 Action: whitelist / blacklist /disable

		Select Mac Option: Any/Other Valid Mac Address: 00:00:00:00:00:06 Valid Mac Mask: 00:00:00:00:00:07 Select IP Option: Any/Other Valid IP Address: 10.0.50.120 2 Valid Mac Mask: 255.255.0.0 Source Port Number: 4
Show	# show acl-settings +----------List 1----------+ Index :4 Profile Name :wagoacl4 Action :whitelist Source Mac :00:00:00:00:00:06 Mask of Source Mac :00:00:00:00:00:07 Source IP :10.0.50.120 Mask of Source IP :255.255.0.0 Source Port :Port4 +----------List 2----------+ Index :5 Profile Name :wagoacl5 Action :whitelist Source Mac :00:00:00:00:00:06 Mask of Source Mac :00:00:00:00:00:07 Source IP :10.0.50.120 Mask of Source IP :255.255.0.0 Source Port :Port5	This command is used to view the ACL configured port settings list.
Configure	#acl-delete 5	This command is used to delete the Acl rule in the setting based on index. Example Index:5
Configure	# acl-clearAll yes	This command is used to delete all the Acl rules list in the settings of the device. Note: Confirmation option “yes” to proceed and “no” to discard

3.3.10 Static SAK Settings CLI commands:

Node	Command	Description
Configure	# macsec-settings 7 enable sci 2233 sak 334455	This command is used to configure the SAK Settings (Note:only for port [7~8]) Example: Source Port: 7 SCI : 2233 SAK : 334455
Configure	#macsec-settings 7 disable	Disable the macsec setting for port (Entering the sak and sci is optional)
Show	#show macsec-status +----------Macsec Static SAK Status----------+ Port : Port7 Status : Enabled sci : 2233 sck : 334455 Port : Port8 Status : Disabled sci : sck :	This command is used to view the macsec setting list of the switch.

3.3.11 SNMP Settings CLI commands:

Node	Command	Description
SNMP Global Configure	# snmp-globalActive enable	This command is used to enable and disable the SNMP feature. Example: Active: enable/disable
SNMP Version Configure	# snmp-versionSet 2_V1/V2c/V3	This command is used to set SNMP version the SNMP version Example: Version: None 1_V1/V2c 2_V1/V2c/V3 3_V3
Show SNMP Global Status	#show snmp-status SNMP is Enabled. SNMP Version Status ---------- V1/V2c Enabled V3 Enabled	This command is used to view the SNMP global status and current SNMP version enabled status.
SNMP Community Configure	#snmp-community wago read-write-all	This command is use to set the SNMP community string and permission type. Example: String: Wago Permission: read-all-only/ read-write-all
Show SNMP Community Configure	# show snmp-community Community Name Access right ---------- wago read-write-all	This command is used to view the SNMP community setting list in the device.
Remove SNMP Community Configure	#snmp-community-remove wago	This command is use to remove community in the SNMP community list String: Wago
SNMP Trap Configuration	# snmp-trapAdd 10.0.50.1 102 wago	This command is used to set the SNMP trap configuration. Example: Server IP: 10.0.50.1 Port Number: 102: 10.0.50.1 Port Number: 102 Community String: Wago
Show the SNMP Trap Configuration	show snmp-trap Trap Mode: Trap Sink IP Sink Port Community Name ---------- 10.0.50.50 162 switch	This command is used to view the SNMP trap configuration.
Remove SNMP Trap settings	#snmp-trap-remove 10.0.50.1 102	This command is used to remove the trap setting using the ip address with port number. Example Server Ip : 10.0.50.1 Port Number:102
SNMP Trap Mode Configure	#snmp-mode Trap	This command is used to set the SNMP Trap mode Example:

		Mode: Trap/Inform
SNMPV3 Auth Configure	# snmp-authV3 user 12345678 123345678	This command is used to set SNMPV3 Auth configuration password and Encryption key (Note length should be 8 to 32) Name: user/admin Password: 12345678 Encryption Key: 12345678
Show SNMPV3 Auth Configure	show snmp-v3auth User Name Authentication Type Data Encryption Type ---------- user MD5 DES admin MD5 DES	This command is to view the SNMP V3 Auth list.
Remove SNMPV3 Auth	# snmp-removeAuthV3 user	This command is used to delete the SNMPv3 user using username. Example: Name: user

3.3.12 SNTP Setting CLI commands:

Node	Command	Description
SNTP Manual Configure	#sntp manual 2021 08 31 11 09 30	This command is used to set the SNTP manually setting date & time. Example: Year: 2021 <1970 ~ 2038> Month: 08 <1 ~ 12> Days: 31 <1 ~ 31> Hours: 11 <0 ~ 23> Minutes: 09 <0 ~ 59> Seconds: 30 <0 ~ 59>
SNTP NTP Server Manually Configure	# sntp ntp-server server-manual ip 10.0.50.120 60 34	This command is used to set the SNTP NTP server manually. Example: NTP Server Selection: ip/domain Server IP: 10.0.50.120 Query Period: 60 Time zone: 34
SNTP NTP Server Select Configure	#sntp ntp-server server-public ntp0.fau.de 60 32	This command is used to set the SNTP NTP server by select. Example: Server IP: ntp0.fau.de / ntps1-1.cs.tu-berlin.de Query Period: 60 Time zone: 34
SNTP DayLight Active Set Configure	#sntp daylight-active enable	This command is used to set the SNTP DayLight Activate set. Example: Active: enable/disable
SNTP DayLight Start Set Configure	#sntp daylight-start Jly 4th Sun 23	This command is used to set the SNTP DayLight start time setting. (Condition: DayLigh should enabled) Example: Month: Jly Week: 4th Day: Sunday Hour: 23

SNTP DayLight End Set Configure	#sntp daylight-end Dec 2nd Fri 20	This command is used to set the SNTP DayLight end time setting. (Condition: DayLigh should enabled) Example: Month: Dec Week: 2nd Day: Friday Hour: 20
Show SNTP	# show sntpStatus SNTP : Disabled NTP Server 1 : time-A.timefreq.bldrdoc.gov Time Zone : 23 Time Server Query Period: 60	This command is used view the current setting of SNTP.

3.3.13 System Information CLI commands:

Node	Command	Description
Show	# show system-information +----------System Information----------+ Model Name : EHG2408 MAC Address : 00:60:E9:26:2F:E4 Application Version : 2.54-svn795 Kernel Version : 2.54-svn795 IP Address : 10.0.50.1 Default Gateway : 10.0.50.254 Subnet Mask : 255.255.255.0	This command is used to view the system information
System Command	# # system-reboot	This command is used to reboot the device. Note : Confirmation option “yes” to proceed and “no” to discard
Configure system reset to default	# reset-default yes	This command is used to set the default setting of the device. Note : 1. Confirmation option “yes” to proceed and “no” to discard 2. Reboot the system to deflect the default setting is mandatory.

3.3.14 Management VLAN ID Setting CLI commands:

Node	Command	Description
Management Vlan ID Config	# vlan-managementId 1	This command is used to set the management VLAN id of the system
Show Management Vlan ID	# show vlan-managementId ---------- Management VLAN ID : 1 ----------	This command is used to view the management VLAN id of the system

3.3.15 RSTP Setting CLI commands:

Node	Command	Description

RSTP Enable Configure	# rstp globalActive enable priority 0	This command is used to enable and set the RSTP priority Example: Set Active: enable/disable Priority: 32768
RSTP Disable Configure	# rstp globalActive disable	This command is used to disable the RSTP. Note: Priority Not required for disable, it is optional
RSTP Port Parameter Configure	# rstp port-settings 4 enable enable enable enable enable	This command is used to set the RSTP port Parameter settings. Example: Port Number: 4 Edge Port : enable/disable RSTP Per Port : enable/disable BPDU Filter : enable/disable BPDU Guard: enable/disable Root Guard: enable/disable
Show RSTP settings	# show rstp | Port | Role | Status | Edge | RSTP | BPDU | BPDU | Root | Port (Fact) Per Por Filter Guard Guard ----------+---------- 1 Designated Disc Not edge Disable Disable Disable Disable 2 Disabled Disc Not edge Disable Disable Disable Disable 3 Disabled Disc Not edge Disable Disable Disable Disable 4 Disabled Disc Edge Disable Enable Enable Enable 5 Disabled Disc Not edge Disable Disable Disable Disable 6 Disabled Disc Not edge Disable Disable Disable Disable 7 Disabled Disc Not edge Disable Disable Disable Disable 8 Disabled Disc Not edge Disable Disable Disable Disable	This command is used to view the current settings of RSTP of the system.

4 Glossary

Term	Description
802.1	A working group of IEEE standards dealing with Local Area Network.
802.1p	Provide mechanism for implementing Quality of Service (QoS) at the Media Access Control Level (MAC).
802.1x	IEEE standard for port-based Network-Access Control. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN
Broadcast	Broadcast packets to all stations of a local network.
Client	Device that use services provided by other participants in the network.
DES	Data Encryption Standard is a block cipher that uses shared secret encryption. It's based on a symmetric-key algorithm that uses a 56-bit key.
DHCP	Dynamic Host Configuration Protocol allows a computer to be configured automatically, eliminating the need for intervention by a network administrator. It also prevents two computers from being configured with the same IP address automatically. There are two versions of DHCP; one for IPv4 and one for IPv6.
DNS	Domain Name System is a hierarchical naming system built for any computers or resources connected to the Internet. It maps domain names into the numerical identifiers. For example, the domain name www.google.com is translated into the address 74.125.153.104.
EAP	Extensible Authentication Protocol is an authentication framework widely used by IEEE.
Ethernet	In star-formed physical transport medium, all stations can send data simultaneously. Collisions are detected and corrected through network protocols.
Gateway	Provide access to other network components on the OSI layer model. Packets which are not going to a local partner are sent to the gateway. The gateway takes care of communication with the remote network.
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol is used on IPv4 networks for establishing multicast group memberships.
IP	Internet Protocol
IPv4	Internet Protocol version 4 is the fourth revision of the Internet Protocol. Together with IPv6, it is the core of internet network. It uses 32-bit addresses, which means there are only 2^32 possible unique addresses. Because of this limitation, an IPv4 addresses became scarce resource. This has stimulated the development of IPv6, which is still in its early stage of development.
LAN	Local Area Network is the network that connects devices in a limited geographical area such as company or computer lab.
MAC	Media Access Control is a sub-layer of the Data Link Layer specified in the OSI model. It provides addressing and channel access control mechanisms to allow network nodes to communicate within a LAN.

MAC Address	A unique identifier assigned to network interfaces for communications on a network segment. It is formed according to the rules of numbering name space managed by IEEE.
MD5	Message-Digest algorithm 5 is a widely used cryptographic which has a function with a 128-bit hash value.
Multicast	This type of transmission sends messages from one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. Also, networks that support multicast send only one copy of the information across the network until the delivery path that reaches group members diverges. At these diverges points, multicast packets will be copied and forwarded. This method can manage high volume of traffic with different destinations while using network bandwidth efficiently.
OSI Model	Open System Interconnection mode is a way of sub-dividing a communication system into smaller parts called layers. A layer is a collection of conceptually similar functions that provide services to the layer above it and receives services from the layer below it.
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service is an authentication and monitoring protocol on the application level for authentication, integrity protection and accounting for network access.
Server	Devices that provide services over the network.
SMTP	Simple Mail Transfer Protocol (SMTP) is an internet standard for email transmission across IP network.
SNMP	Simple Network Management Protocol is a protocol for managing devices on IP networks. It exposes management data in the form of variables on the managed systems, which describe the system configuration.

Atop Technologies, Inc.

www.atoponline.com
www.atop.com.tw

TAIWAN HEADQUARTER:

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City, Hsinchu County
Taiwan, R.O.C.
Tel: +886-3-550-8137
Fax: +886-3-550-8131

ATOP CHINA BRANCH:

3F, 75th, No. 1066 Building,
Qingzhou North Road,
Shanghai, China
Tel: +86-21-64956231

ATOP INDIA OFFICE:

Abhishek Srivastava
Head of India Sales
Atop Communication Solution(P) Ltd.
No. 22, Kensington Terrace,
Kensington Rd,
Bangalore, 560008, India
Tel: +91-80-4920-6363
E-mail: Abhishek.S@atop.in

ATOP INDONESIA BRANCH:

Jopson Li
Branch Director
Wisma Lampung Jl.
No. 40, Tomang Raya
Jakarta Barat, 11430, Indonesia
Tel. +62-857-105957755
E-mail : jopsonli@atop.com.tw

ATOP EMEA OFFICE:

Bhaskar Kailas (BK)
Vice President (Business Development)
Atop Communication Solution(P) Ltd.
No. 22, Kensington Terrace,
Kensington Rd,
Bangalore, 560008, India
Tel: +91-988-0788-559
E-mail: Bhaskar.k@atop.in

ATOP AMERICAs OFFICE:

Venke Char
Sr. Vice President & Head of Business
11811 North Tatum Blvd, Suite 3031
Phoenix, AZ 85028,
United States
Tel: +1-602-953-7669
E-mail: venke@atop.in